République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Mouloud Mammeri de Tizi-Ouzou
Faculté de génie éléctrique et d'informatique

Mémoire

En vue de l'obtention du diplôme

De master en Informatique

Option : Ingénierie des systèmes d'informations

Thème

Sécurité et cryptage des données
Cas de la machine Enigma

Dirigé par :

M^{r} Chaieb Yazid

Réalisé par :

M^{elle} : Dorbane Hayat
M^{elle} :Khalef Tassaadit

Promotion : 2014/2015

Sommaire

La liste des figures

La liste des tableaux

Introduction générale

Depuis l'antiquité l'homme est préoccupé par la problématique de sécurité sous toutes les formes, et le mystère suscite un vif intérêt chez l'homme, tout se qui est caché l'attire. Ceci n'est que logique car ne dit on pas que celui qui sait détient un quelconque pouvoir, celui qui dissimule en détient un tout aussi grand.

Aujourd'hui, il est souvent indispensable de cacher certaines choses. Et a tous les niveaux, il semble important d'empêcher le premier venu d'accéder a certaines informations La volonté de crypter se trouve partout : les banques ou les industries…..il s'est donc développé des techniques pour rendre les documents illisible : les algorithmes cryptage ou crypto système.

Les deux mots grecs 'kryptos'qui signifie 'caché' et' graphien' qui veux dire 'écrire' sont à l'origine du mot cryptographie, qui se traduise en 'écrire en cacher 'ou 'écriture cachées'

Des procédés cryptographiques existent depuis toujours et l'époque moderne n'a fais que les affiner grâce au développement des mathématiques et des sciences informatiques.
Les services secrets on utilisé toutes sortes d'encodage pour transmettre des informations entre agents et gouvernements, de telle sorte que les ennemi potentiels ne puissent les utiliser. La cryptographie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Ainsi, très peu de gens, voire personne n'utilisait la cryptographie a des fins personnelles. C'est pourquoi, pendant tant d'années, elle est restée une science discrète.

Aujourd'hui la cryptographie est science a part entière accessible à tous. En effet, de nos jours toutes personne désirant confidentialité des informations peut soit concevoir son propre crypto- système, se servir de ceux déjà existant.

Bien que les lois sur de cryptage de données soient quelques fois très strictes dans certaine pays, cela n'empêche pas les gens d'y avoir recours même si pour cela il faut chiffrer en cachette.

Plusieurs crypto systèmes et techniques sont disponible sur le marché et surtout sur le net. Actuellement, les deux techniques de cryptage les plus utilisées sont : le cryptage symétrique et cryptage asymétrique.
Dans cette étude, nous allons essayer d'expliquer ces deux techniques en les illustrant par
Quatre chapitres sont consacres a ce travail :

Apres l'introduction générale, on à traité dans le premier chapitre les systèmes d'informations et la sécurité des informations en général.

Le second chapitre dans lequel on trouve des généralités liées a la cryptographie .Ces généralités consistent en certains nombres d'aspects liés a l'évolution de la cryptographie a travers le temps.

Le troisième chapitre est scindé en deux parties :

Dans la première, nous étudierons deux algorithmes de chiffrement symétriques, à savoir le DES (Data Encryptions Standard) et AES (Advanced Encryptions Standard), ainsi un algorithme de chiffrement asymétrique et une fonction de hachage, qui sont respectivement : le RSA et le MD5.Enfin nous avons fait une brève étude comparative des deux méthodes de chiffrement cités précédemment.

Dans la deuxième partie, on fera une simple étude de la machine enigma :son histoire, sa composition et son fonctionnement.

En dernier chapitre : nous allons présenter les interfaces graphiques qui décrivent le fonctionnement de notre application.

1.1. Les systèmes d'information :

Définition :

Dans la littérature, plusieurs définitions du système d'information sont formulées, mais d'une manière générale, un système d'information regroupe l'ensemble des informations manipulées sous toutes leurs formes dans une organisation. Une partie seulement donnera lieu à un traitement automatisé, on parlera alors de système d'information automatisé (S.I.A.) qu'il faut situer par rapport à l'ensemble du système d'information.

J.L. Peaucellenous donne une définition qui présente les objectifs liés au système d'information en terme de sécurité (fiabilité et objectivité), de délais (rapidement), de diminution des coûts (économiquement), d'organisation (efficacité des actes des organisations) : "le système d'information est un langage de communication de l'organisation, construit consciemment pour représenter de manière fiable et objective, rapidement et économiquement, certains aspects de son activité, passée ou à venir. Les phrases et les mots de ce langage sont les données dont le sens vient des règles de leur élaboration, par des hommes ou par des machines. Les mécanismes de représentation propre à ce type de langage prennent leur efficacité dans la répétitivité des actes des organisations.

Cette définition suggère que chaque praticien doit s'assurer lors de la conception que les objectifs assignés au système d'information correspondent aux objectifs énumérés par J.L. Peaucelle. G.Davis dans son ouvrage, propose une définition qui décrit la structure physique d'un système d'information : " un système d'information de gestion est un système machine intégré qui produit de l'information pour assister les êtres humains dans les fonctions d'exécution, de gestion et de prise de décision. Le système utilise des équipements informatiques et des logiciels, des bases de données, des procédures manuelles, des modèles pour l'analyse, la planification, le contrôle et la prise de décision ".

- **Entrées :** Les entrées représentent toutes les données, textes, sons et images entrant dans le S.I. et les méthodes et les moyens avec lesquels ces entrées ont été collectées et entrées.
- **Modèles :** Cette structure représente une combinaison de modèles procéduraux (transaction homme- machine), logiques (modèle logique ou interne de données) et mathématiques (Maths, Recherche opérationnelle,...etc.) qui manipulent les entrées

et les données stockées sous diverses formes pour produire les résultats désirés ou les sorties.

- **Technologies :** La technologie (le logiciel, le matériel et le papier) est la boite à outils du travail du SI. Elle capture les entrées, conduit les modèles, enregistre et accède aux données, produit et transmet les sorties.

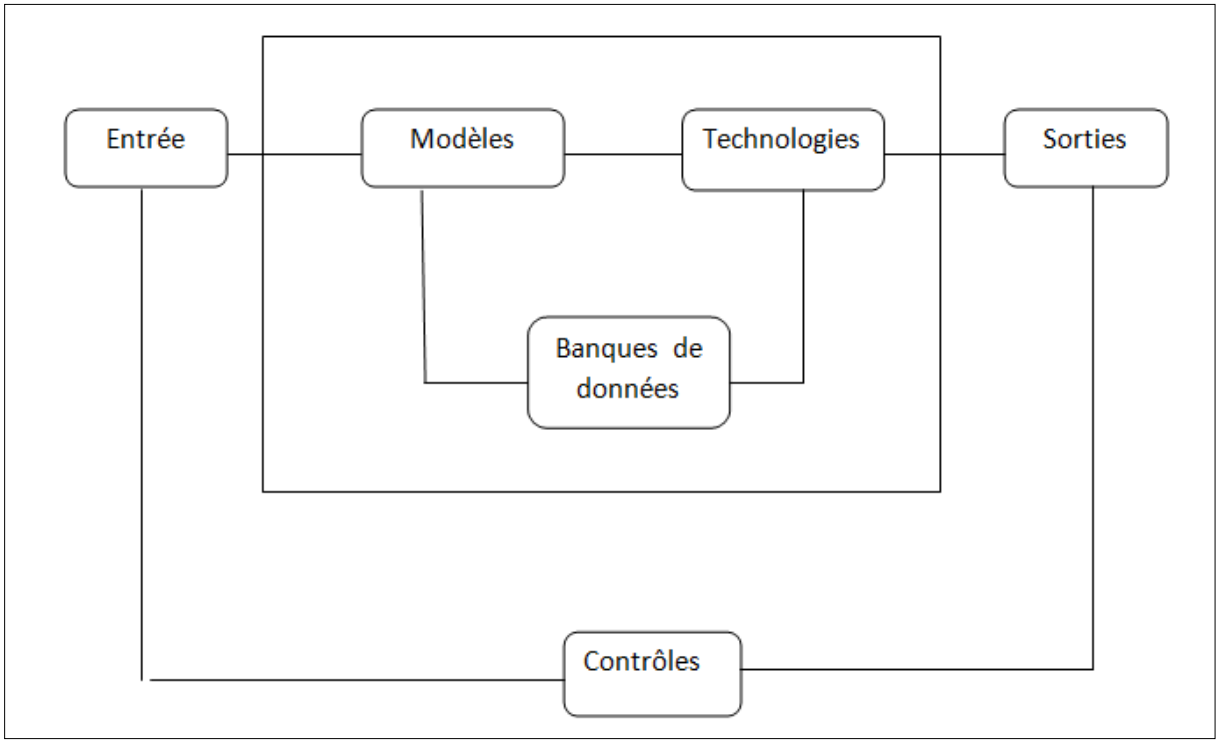


Figure 1: Structure physique de système d'information.

- **Base de données :** La base de données est le moyen ou sont emmagasinées toutes les informations nécessaires à tous les utilisateurs.
- **Contrôles :** Tout S.I. se trouve confronté à une variété d'incidents, toute sécurité efficace passe par une étude de risques volontaires ou accidentels.
- **Sorties :** Le produit du S.I. est la sortie d'informations de qualité pour tout utilisateur intra ou extra organisation. La qualité spécifie la fiabilité, l'opportunité et la concision de l'information en sortie.

1.2. Définition de la sécurité des systèmes d'informions : [01]

Le terme sécurité dépend du contexte ou il est utilisé, par exemple, la sécurité d'un véhicule. D'un point de vue, la sécurité d'une voiture est principalement concentrée sur la sûreté des personnes à l'intérieur de la voiture, d'un autre point de vue, la sécurité d'une voiture peut être contre les voles.

La sécurité est souvent interprétée de manière subjective, elle correspond à une protection qui n'est pas forcement la même pour tous, en effet, elle change en fonction de ses besoins.

Cependant dans le contexte de la sécurité des systèmes d'information, il convient de matérialiser objectivement la notion de la sécurité. La sécurité des systèmes d'information n'est qu'une partie de la sécurité des informations. Les informations existent à l'intérieur comme a l'extérieur d'un ordinateur et doivent être protégées chaque fois qu'elles soient utilisées, transmises la sécurité des systèmes d'information traite en premier lieu et essentiellement les informations et leurs traitements.

Historiquement, la sécurité des systèmes d'information est une variante de la sécurité informatique. La sécurité informatique qui a constitué une préoccupation ancienne, elle a été longtemps intégrée dans les systèmes d'exploitation, cœur logiciel des ordinateurs. Elle a constitué un besoin particulièrement fort pour les secteurs critiques (banques, défense,…etc.).

- **La sécurité informatique** *:* est la capacité d'un système de protéger ses objetscontre leur modification ou leur utilisation par des sujetsnon autorisés.

Avec l'apparition des réseaux ouverts, la généralisation d'Internet, un nouveau contexte pour lequel la sécurité a pris une dimension plus globale : la sécurité des systèmes d'information.

- **La sécurité des systèmes d'information :**recouvre l'ensemble des méthodes, techniques et outils mis en œuvre pour protéger les ressources d'un système d'information contre les sinistres, les erreurs et les malveillances de façon à rendre leur probabilité et/ou leur conséquence compatible avec les exigences de sécurité dégagées. Autrement dit, assurer la sécurité d'un système d'information revient à garantir les facteurs de base de la sécurité suivante :

- La confidentialité,
- L'intégrité
- La disponibilité.

1. La confidentialité:

La confidentialité**,** propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés. Exprimer les besoins de confidentialité, c'est déterminer les utilisateurs autorisés et la limite de leurs prérogatives

Formuler des exigences en matière de confidentialité d'une information revient à énoncer des critères sur lesquels se fonde la légitimité des accès à cette information, par exemple**:**

- Critères liés à la personne : identité, appartenance à un groupe, habilitation…etc.
- Critères liés à la fonction : droits, autorisations, besoin d'en connaître, besoin d'en user,…etc.
- Critères liés à un rôle : responsabilités, délégations, nécessités,…etc.

2. L'intégrité :

L'intégrité, une propriété assurant que des ressources de système (ressource englobe même les informations) n'ont pas été modifiées ou détruites de façon non autorisée. Ce facteur garantit que les systèmes et les informations traités ne sont modifiés que par une action volontaire et légitime. L'intégrité consiste à assurer un maintient correct entre les relations spécifiques des différentes données et l'échange des données entre utilisateurs ou processus sans avoir subi d'altération. L'intégrité regroupe un ensemble de fonctions, par exemple:

- Les fonctions destinées à garantir que des données n'ont pas été modifiées d'une manière non autorisées,
- Les fonctions permettant de déceler ou d'empêcher toute perte, ajout ou modification lorsque les données sont échangées,
- Les fonctions interdisant la modification de la source ou de la destination du transfert de données.

3. La disponibilité

La disponibilité de service est la prévention d'un déni non autorisé d'accès à l'information (ressources au sens plus général). Elle doit pouvoir garantir, d'une part, que les tâches critiques en temps sont exécutées au moment voulu et que, d'autre part, les tâches non critiques ne puissent pas le devenir. Il s'agit également de garantir que l'accès aux ressources est possible quand on en a besoin, et que les ressources ne sont pas sollicitées ou conservées inutilement. La disponibilité du service peut s'exprimer sous diverses formes, par exemple :

- Délais de réponse.
- Continuité de service.

1.3. La Sécurité et la qualité des systèmes d'information : [02]

Dans les différentes approches sur la spécification de la qualité des systèmes d'information, les graphes de Boehm et de Mc Call sont parmi les plus connus et les plus faciles à exploiter.

Cependant, vue le domaine de la spécification de la qualité des systèmes d'information (un sujet qui mérite lui même un chapitre à part), il paraît plus intéressant et pratique d'en faire une interprétation synthétique et par conséquent de proposer un modèle limité, mais plus pratique d'emploi dans notre contexte.

Comme résultat de synthèse, nous pouvons classer les différents facteurs dans deux rubriques, d'une part les facteurs de qualité d'exploitation (utilisation courante) du système d'information, et d'autre part les facteurs de qualité de son évaluation, cette dernière rubrique est à exclure, vu le contexte de notre projet, elle reflète la maintenance (système maintenable, capable à encaisser des adaptations d'évaluation et/ou de correction).

Pour les facteurs relatifs à la qualité de service (exploitation) du système d'information, nous citons :

- La disponibilité,
- La fiabilité,
- La sûreté,
- L'intégrité,
- L'efficacité,
- La maniabilité.

- **La disponibilité** d'un système est définie comme la probabilité qu'il soit opérationnel à l'instant T, en d'autres termes, c'est le pourcentage de bon fonctionnement (l'exécution de ses fonctions) pendant sa vie opérationnelle. La même définition pour la disponibilité des informations de système. La perte de disponibilité désignée souvent sous le nom du démenti du service.
- **La fiabilité** d'un système est la probabilité qu'il exécutera ses fonctions pendant une période de temps (un intervalle de temps). La fiabilité prend un sens plus large que la disponibilité puisque la fiabilité est une mesure de la continuité d'un service pendant une période bien précise.

- **La sûreté** d'un système d'information est la probabilité de son bon fonctionnement pendant son exécution, en toutes circonstances, ce qui va au delà de la fiabilité qui représente une sûreté limité à une durée définie à l'avance ou statique.
- **L'intégrité** de tout le système y compris ses ressources. Les informations sont accessibles exclusivement par ceux auxquels elles sont destinées et protégées contre les actes des malveillants.
- **L'efficacité**, le système économe des ressources sollicitées en exploitation et disposant d'un bon équilibre qualité/coût.
- **La maniabilité**, le système facile d'emploi et convivial pour l'utilisateur, il est apte à communiquer avec les autres systèmes.

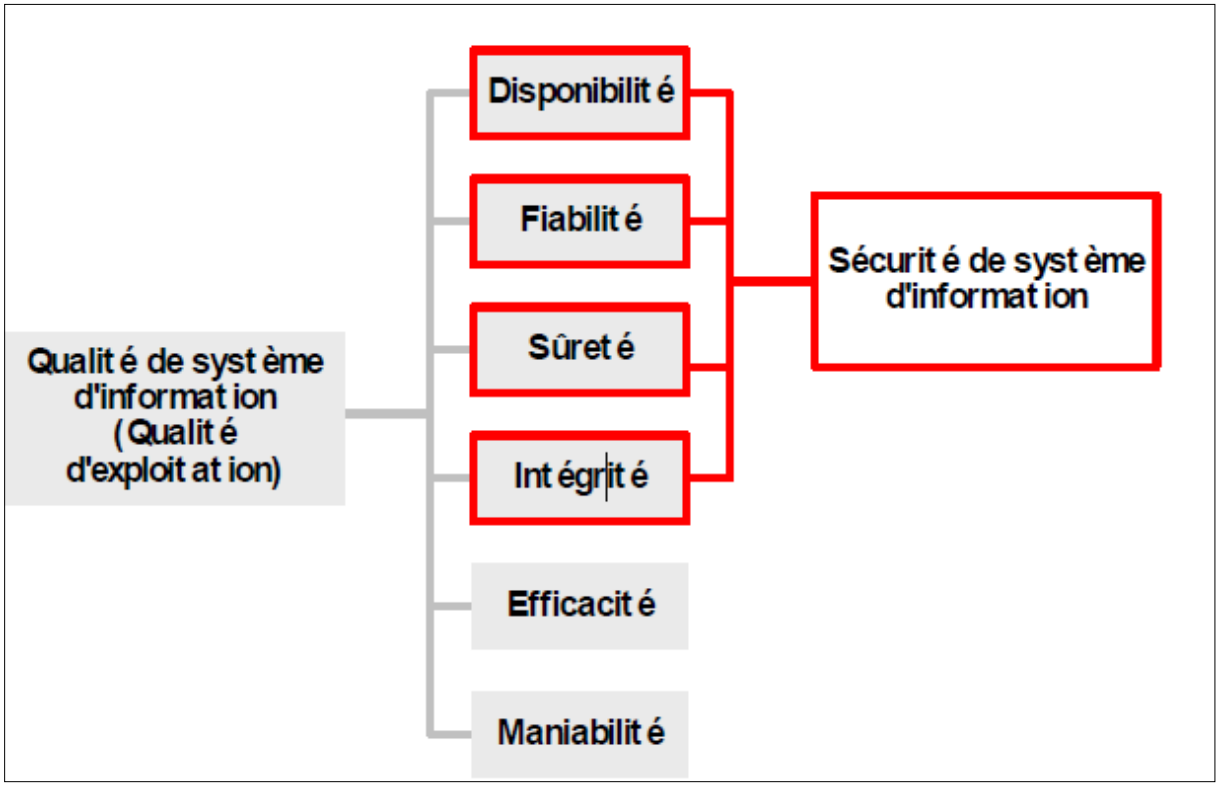


Figure 2 : La position de la sécurité dans la qualité des systèmes d'information.

En analysant ces principaux facteurs de qualité de SI de point de vue de la sécurité. Nous trouvons qu'elle englobe à la fois : la disponibilité, la fiabilité, la sûreté et l'intégrité. Autrement dit, la sécurité d'un système d'information représente un élément crucial dans la qualité de l'exploitation du système (**Figure 2)**

1.4. Terminologies de la sécurité des systèmes d'information :[03]

❖ Vulnérabilité

C'est une faiblesse, une faille dans les mesures de protection ou encore dans l'absence de mesures de protection et de contrôles (physique ou autres) qui peuvent être exploitées par une menace. Elles sont souvent interprétées par l'absence de mesure de protection.

Une vulnérabilité est difficile à détecter, même pour les spécialistes. Il existe des organismes spécialisés pour l'identification des vulnérabilités**.** Des listes de vulnérabilités classées par domaine (organisationnel, matériel,…etc.) existent, tels que, les listes des vulnérabilités des systèmes d'exploitation proposées par les CERT, le CSI et bien d'autres.

Les vulnérabilités existent dans le matériel et dans le logiciel, dans les règles et dans les procédures et aussi parmi le personnel. Tout ce qui peut être exploité pour obtenir un avantage non accordé est une vulnérabilité. Nous proposons les quelques une des causes de vulnérabilités les plus courantes :

- Vulnérabilité de matériel : disque dur, périphériques,…etc.
- Vulnérabilité de logiciel : les systèmes d'exploitation et les applications.
- Vulnérabilité d'infrastructure : réseau de communication hors service.
- Vulnérabilité des processus de contrôle : les règles de sécurité sont mal interprétées ou mal implémentées.

❖ Menace :

Une menace est une source de danger pour le système et se traduit par la présence d'une violation potentielle de la sécurité. Cela peut être une personne, une chose, un événement ou une idée qui constitue un danger à un patrimoine en termes de confidentialité, d'intégrité, de disponibilité et d'utilisation approuvée du système. Toute menace est une cause potentielle de perte. La notion de menace ne saurait être isolée de celle de vulnérabilité, mais contrairement à cette dernière, les responsables de la sécurité n'ont pas d'influence sur les menaces, mais ils peuvent se protéger en agissant sur ses potentielles vulnérabilités dans le système. La dimension et le type des menaces dépendent de la dimension et la complexité du système d'information et de niveau de la technologie mise en œuvre

Les systèmes d'information doivent faire face à une grande variété de menaces, parmi lesquelles nous trouverons le crime informatique, l'espionnage, les accidents, les désastres naturels,...etc.

A ce niveau, il reste à signaler qu'au fur et à mesure que s'accroît la dépendance de l'activité vis à vis de l'information (le cas des systèmes d'information), les menaces augmentent quantitativement, deviennent plus ambitieuses et leur complexité s'intensifie, elles peuvent êtres classées en deux catégories : accidentelles et intentionnelles.

a)Les menaces accidentelles : ou non intentionnelles qui peuvent être réalisées par une exposition ou une modification des informations. Par exemple :

- L'erreur humaine, ce type d'erreur est de loin la menace la plus répondue contre les ressources d'un système d'information, ce sont les utilisateurs autorisés commettant des erreurs susceptibles de causer des pertes.
- Panne du système informatique, le système informatique comprend du matériel, du logiciel et une infrastructure, et ces composants sont toutes susceptibles de pannes à des degrés divers

b) Les menaces intentionnelles : qui correspondent aux attaques dont le but est de violer la sécurité du système. Par exemple :

- Actes de malveillance : les actes de malveillances sont le fait d'individus ou de groupe d'individus qui visent tel ou tel système particulier, exemple les hackers, des espions industriels,…etc.
- Logiciels malveillants : nous désignons sous ce nom des logiciels créant ou exploitant une vulnérabilité. Ce sont des outils pouvant être utilisés de façon constructive ou destructive.

Par exemple :

a) Attaques par débordement de tampon (buffer overflow) :

- *Introduction au buffer overflow :*

Les attaques par « débordement de tampon » (en anglais « Buffer overflow », parfois également appelées dépassement de tampon) ont pour principe l'exécution de code arbitraire par un programme en lui envoyant plus de données qu'il n'est censé en recevoir. En effet, les programmes acceptant des données en entrée, passées en paramètre, les stockent temporairement dans une zone de la mémoire appelée tampon (en anglais buffer). Or,

certaines fonctions de lecture, telles que les fonctions strcpy() du langage C, ne gèrent pas ce type de débordement et provoquent un plantage de l'application pouvant aboutir à l'exécution du code arbitraire et ainsi donner un accès au système. La mise en oeuvre de ce type d'attaque est très compliquée car elle demande une connaissance fine de l'architecture des programmes et des processeurs. Néanmoins, il existe de nombreux exploits capable d'automatiser ce type d'attaque et la rendant à la portée de quasi-néophytes.

- *Principe de fonctionnement :*

Le principe de fonctionnement d'un débordement de tampon est fortement lié à l'architecture du processeur sur lequel l'application vulnérable est exécutée. Les données saisies dans une application sont stockée en mémoire vive dans une zone appelée tampon. Un programme correctement conçu doit prévoir une taille maximale pour les données en entrées et vérifier que les données saisies ne dépassent pas cette valeur. Les instructions et les données d'un programme en cours d'exécution sont provisoirement stockées en mémoire de manière contigûe dans une zone appelée pile (en anglais stack). Les données situées après le tampon contiennent ainsi une adresse de retour (appelée pointeur d'instruction) permettant au programme de continuer son exécution. Si la taille des données est supérieure à la taille du tampon, l'adresse de retour est alors écrasée et le programme lira une adresse mémoire invalide provoquant une faute de segmentation (en anglais segmentation fault) de l'application. Un pirate ayant de bonnes connaissances techniques peut s'assurer que l'adresse mémoire écrasé corresponde à une adresse réelle, par exemple située dans le tampon lui-même. Ainsi, en écrivant des instructions dans le tampon (code arbitraire), il lui est simple de l'exécuter.

Il est ainsi possible d'inclure dans le tampon des instructions ouvrant un interprêteur de commande (en anglais shell) et permettant au pirate de prendre la main sur le système. Ce code arbitraire permettant d'exécuter l'interprêteur de commande est appelé shellcode.

- *Se protéger d'un Buffer overflow :*

Pour se protéger de ce type d'attaque, il est nécessaire de développer des applications à l'aide de langages de programmation évolués, assurant une gestion fine de la mémoire allouée ou bien à l'aide de langage de bas niveau en utilisant des bibliothèques de fonctions sécurisées (par exemple les fonctions strncpy()). Des bulletins d'alerte sont régulièrement publiés, annonçant la vulnérabilité de certaines applications à des attaques par débordement de tampon. Suite à ces bulletins d'alerte, les éditeurs des logiciels touchés par la vulnérabilité publient généralement des correctifs (patchs) permettant de corriger la faille. Tout

administrateur système et réseau se doit de se tenir informé des alertes de sécurité et d'appliquer le plus rapidement possible les correctifs.

b) L'attaque stackoverflow :

Un dépassement de pile ou débordement de pile (en anglais, ***stackoverflow***) est un bug causé par un processus qui lors de l'écriture dans une pile, écrit à l'extérieur de l'espace alloué à la pile, écrasant ainsi des informations nécessaires au processus.

L'expression *dépassement de pile* peut s'appliquer à toutes les piles. Cependant, lorsque l'on parle de dépassement de pile, on fait habituellement référence à la piled'exécution. Il serait alors plus précis de dire dépassement de la pile d'exécution, mais les informaticiens ont pris l'habitude de dire simplement dépassement de pile lorsque le contexte indique que la pile dont on parle est la pile d'exécution.

c) Virus :

Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé. La définition d'un virus pourrait être la suivante : « Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire. » Le véritable nom donné aux virus est CPA soit Code Auto-Propageable, mais par analogie avec le domaine médical, le nom de "virus" leur a été donné. Les virus résidents (appelés TSR en anglais pour Terminate and stayresident) se chargent dans la mémoire vive de l'ordinateur afin d'infecter les fichiers exécutables lancés par l'utilisateur. Les virus non résidants infectent les programmes présents sur le disque dur dès leur exécution.

d) **Les vers** :

Sont des virus capables de se propager à travers un réseau.

e) **Les chevaux de Troie** :

On appelle « **Cheval de Troie** » (en anglais trojan horse) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur.

- Principe :

Le principe des chevaux de Troie étant généralement (et de plus en plus) d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine par le port qu'il a ouvert.

Toutefois pour pouvoir s'infiltrer sur votre machine, le pirate doit généralement en connaîtrel'adresse IP. Ainsi :

- soit vous avez une adresse IP fixe (cas d'une entreprise ou bien parfois de particuliers connecté par câble, etc.) auquel cas l'adresse IP peut être facilement récupérée
- soit votre adresse IP est dynamique (affectée à chaque connexion), c'est le cas pour les connexions par modem ; auquel cas le pirate doit scanner des adresses IP au hasard afin de déceler les adresses IP correspondant à des machines infectées.

f) Les bombes logiques :

Sont appelés bombes logiques les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système. Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de bombe à retardement ou de bombe temporelle), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

g) Spoofing :

Méthode d'usurpation de l'identité d'une machine. Le spoofing peut porter sur l'adaptation de l'adresse IP,l'adresse MAC ou tout autre élément permettant d'identifier une machine sur un réseau, afin de pouvoir se faire passer pour la machine usurpée et agir soit en son nom pour atteindre des niveaux de privilèges et d'accès non autorisés autrement soit agir pour lui porter atteinte comme dans le cas d'attaques de type smurfing.

h) Sniffer :

Logiciel qui permet d'intercepter des données transitant sur un réseau. Les pirates utilisent ce type d'outils afin de récupérer à l'insu des utilisateurs et des administrateurs réseaux des informations sensibles et confidentielles qui traversent les réseaux telles que les couples identifiants/mots de passe. Le sniffing est un processus de collecte d'information dit passif puisque le pirate n'entre pas en communication directe avec lesmachines dont il renifle et voit passer les données.

❖ **Les attaques :**

C'est l'action entreprise par un objet (individu ou programme) pour modifier l'état d'un système. Une attaque peut aboutir en exploitant les vulnérabilités du système, elle concrétise une menace. Elle peut être directe auquel cas elle s'adresse à la ressource ciblée ou indirecte où elle obtient des informations d'une autre ressource sans attaquer la ressource ciblée directement :

- **Passive :** elle consiste à observer le système pendant son exploitation et collecter des informations, par exemple l'analyse et la surveillance des communications non protégée et la capture d'information d'authentification (telle que des mots de passe). Ce type d'attaque est difficile à détecter.
- **Active** : elle change le comportement du système pour abuser délibérément du système.

❖ **Les risques :**

Le Robert définit le risque comme étant "l'éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage". C'est un concept bien ancien que les systèmes d'information. Il est largement abordé dans les ouvrages du management des projets. Dans notre contexte, en système d'information le risque est la conjonction d'une menace et d'une vulnérabilité dans un système ; celle-ci générant un risque et pouvant produire d'éventuelles pertes, c'est la mesure du coût des conséquences d'une attaque, il prend en compte la probabilité de succès de l'attaque. La conception d'une politiquede sécurité d'un système d'information passe obligatoirement par une étape d'analyse des risques menaçant la sécurité. L'analyse du risque identifie les besoins en sécurité ainsi que les menaces. Les risques potentiels qui pèsent sur les systèmes d'information peuvent prendre une multitude de forme. Plusieurs typologies des risques existent :

- Des risques internes et externes ;
- Des risques matériels et immatériels ;
- Des risques organisationnels, humains, juridiques, techniques ;
- Des risques liés aux personnes, aux procédures, aux protocoles et aux matériels;
- Des risques prévisibles ou imprévisibles;
- Des risques maîtrisables ou non.

A partir de là, nous pouvons conclure que les risques liés aux systèmes d'information sont des risques au même titre que les autres risques des organisations.

En plus ces risques varient selon les besoins selon les besoins et le contexte de l'utilisation des systèmes d'informations, ils sont en relation forte avec le secteur d'activité de l'organisme en général

- La taille de l'organisme.
- L'image de l'organisme.
- Dépendance de l'organisme vis-à-vis de système d'information.

❖ Service de sécurité

Services de sécurité ou (mesures de protection ou Safeguards), C'est l'ensemble des contrôles physiques, des mécanismes et des procédures pour protéger le patrimoine informationnel et matériel des menaces de sécurité possibles.

Selon, les services de sécurité d'un système d'information peuvent être classés en trois catégories :

- **Le service de détection :**est utilisé pour détecter toutes les tentatives réussies ou non de violation de la sécurité. Nous pouvons citer l'utilisation : Des alarmes pour détecter les accès physiques non autorisés. Des systèmes d'audit pour enregistrer toutes les activités du système et l'exploitation de ces données enregistrées pour détecter des activités inhabituelles ou suspectes.
- **Le service de recouvrement :**utilisé après l'occurrence d'une violation de sécurité pour restaurer le système à son état avant sa violation. Citons l'exemple des sauvegardes de données et des systèmes dupliqués.
- **Les services de prévention** : assurent la sécurité du système au cours de son exploitation en prévenant l'occurrence des violations de sécurité. On peut citer l'exemple du service de cryptage pour prévenir l'accès aux objets du système par des

sujets non autorisés. Les services de détection et de recouvrement sont moins développés que les services de prévention. L'organisation internationale de normalisation (ISO) définit dans ses standards cinq services de sécurité de base qui sont des services de prévention. Il s'agit de :

- **Service d'authentification**: La méthode d'authentification la plus utilisée est basée sur les mots de passe pour identifier les utilisateurs, c'est aussi l'angle d'attaque le plus utilisé contre les systèmes d'information.
- **Service d'intégrité**: L'objectif de ce service est d'assurer l'authenticité et la non divulgation des informations stockées ou échangées à travers un réseau informatique. Par exemple, ce peut utiliser des fonctions de cryptage.
- **Service de confidentialité et d'intégrité**: Le contrôle des accès aux ressources d'un système d'information est justifié par le besoin de vouloir assurer la confidentialité, l'intégrité et la disponibilité des ressources du système.
- **Service de contrôle d'accès.**
- **Service de non répudiation :**Assurer la **non-répudiation** (authenticité de l'acte, sécuriser une transaction commerciale... La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier à la transaction

A ce critère de sécurité sont associées les notions d'imputabilité, de traçabilité et éventuellement d'adaptabilité:

1-L'imputabilité :se définit par l'affectation certaine d'une entité à une action ou à un événement.L'imputabilité est réalisée par l'ensemble des exigences garantissant l'enregistrement des informations pertinentes sur l'individu agissant.

2-Latraçabilité : est la fonction de sécurité qui comprend, le cas échéant, bien évidemment, l'imputation, mais qui mémorise l'origine d'un message, d'un événement, d'une information ou d'une donnée. Elle permet, par exemple, deretrouver l'adresse à partir de laquelle ces données ont été envoyées.

3-L'adaptabilité :se définit par la capacité d'un système à garantir la présence des informations nécessaire à une analyse ultérieure d'un événement (courant ou exceptionnel)

dans le but de déterminer s'il y a effectivement eu violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises. C'est également la fonction destinée à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité.

A partir de la nature des ressources des systèmes d'information, le contrôle d'accès prend diverses formes. Il peut prendre la dimension organisationnelle (accès physique), informationnelle…etc.

1.5. Fonction ou mécanisme de sécurité :

Une fonction ou un mécanisme de sécurité est tout objet utilisé pour fournir un ou plusieurs services de sécurité, par exemple, prenons l'exemple du service d'authentification, nous utilisons un algorithme qui est considéré comme une fonction de sécurité. Au niveau de contrôle d'accès, nous pouvons définir des règles de gestion comme fonction de sécurité.

L'ensemble des mécanismes de sécurité peut être divisé en trois sous ensembles:

- Ensemble des mécanismes garantissant la sécurité logicielle (Information relatedsecurity).
- Ensemble de mécanismes garantissant la sécurité matérielle (Hardware relatedsecurity).
- Ensemble de mécanismes garantissant la sécurité organisationnelle (Administration relatedsecurity).

1) La sécurité logicielle :la sécurité de l'information est la protection des objets contre des vulnérabilités actuelles dans l'architecture du système, c.-à-d. vulnérabilités dans le logiciel, matériel et dans la combinaison du logiciel et du matériel. Elle traite une grande variété de problèmes : comment les programmes à l'intérieur de l'ordinateur devraient agir, d'imposer la politique de sécurité ; comment le mécanisme de contrôle d'accès devrait fonctionner …etc.

2) La sécurité matérielle traite la protection du matériel dans le système contre des menaces physiques externes, telles que le tri fouillage, vol, tremblements de terre, inondation de l'eau. Tout équipement manipulant ou contenant l'information sensible doit être protégée. Il ne doit y avoir aucune possibilité pour qu'un intrus accède à ces dispositifs, par exemple aucune personne ne doit pouvoir enlever un disque contenant l'information sensible ou installer des dispositifs pour enregistrer l'information confidentielle.

3) La sécurité organisationnelle ou la protection des objets contre des vulnérabilités issues des utilisateurs (humains) et des menaces dues aux vulnérabilités dans l'organisation

(procédure). Elle protège les objets (ressources) contre les attaques provenant des utilisateurs autorisés. Elle impose les règles organisationnelles (fonctionnelles) indiquées dans la politique de sécurité, par exemple, les actions à prendre quand des violations de sécurité sont détectées dans le système.

1.6. La politique de sécurité des systèmes d'information :

Une organisation qui possède un système d'information devrait mener une réflexion sur ses attentes et sa dépendance vis-à-vis de l'informatique et sur sa définition d'une utilisation normale des moyens qu'elle met à la disposition des utilisateurs. La politique de sécurité d'un système d'information est l'aboutissement et la synthèse de ces travaux. Selon Olobson, Une politique desécurité spécifie l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les informations et autres ressources sensibles au sein d'un système spécifique, d'une organisation. Une politique de sécurité identifie les objectifs de sécurité, les moyens physiques relatifs au personnel et à l'organisation et les menaces prises en compte par une combinaison de fonctions dédiée à la sécurité**,** implémentée dans une cible de sécurité.

- ***Mise en place d'une politique de sécurité :***

Il nous faut avant tout prendre conscience de la diversité des besoins en matière de sécurité. Chaque ressource du système a des exigences différentes qui, d'une part, dépendent des activités de la ressource dans le système et, d'autre part sont étroitement liées à son environnement.

Ensuite, une politique de sécurité doit être capable de s'interroger dans la culture de l'organisme. Dans le cas contraire, elle risque d'être rejetée par les utilisateurs et son intérêt sera alors significativement rejeté.

La méthodologie de la mise en place d'une politique de sécurité est décrite dans. Celui-ci présente les différentes phases de sa conception ainsi que les entités intervenant à chaque phase, nous pouvons résumer ces différentes phases comme suit :

- L'identification des ressources que nous souhaitons protéger.
- L'identification des risques (risques internes, risques externes,…etc.).
- L'analyse de la probabilité des menaces.
- La définition et la mise en place de solutions avec un souci d'efficacité financière.

Itération de ce processus, afin d'améliorer ou de mettre à jour la politique en fonction des événements (modifications des ressources, faille découverte suite à un événement).

Il reste à signaler que la dimension financière est essentielle, puisqu'un principe de base dans le domaine de la sécurité en général est que le coût des mesures mises en place pour protéger les ressources ne doit pas exercer le coût engendré par l'éventuelle 'destruction' de ces ressources. L'évaluation des besoins réels consiste à pondérer le coût des solutions

1.7. Conclusion :

Un système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, affin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources. Est pour assurer la sécurité on à besoin de crypter les données avec des différentes méthodes telque la cryptographie classique et moderne que nous allons décrire en détail dans le prochain chapitre.

2.1. Introduction à la cryptographie :

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de façon sécuritaire est probablement aussi ancien que les communications elles-mêmes.D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif. Dans notre monde moderne, où diverses méthodes de communication sont utilisées régulièrement, le besoin de confidentialité est plus présent que jamais à une multitude de niveaux. Par exemple, il est normal qu'une firme désire protéger ses nouveaux logiciels contre la piraterie, que les institutions bancaires veuillent s'assurer que les transactions sont sécuritaires et que tous les individus souhaitent que l'on protège leurs données personnelles.

Aussi vous, vous êtes assis à votre bureau et vous devez remplir la tâche plutôtbanale d'envoyer un document commercial à un collègue de telle sorte que personne d'autre ne puisse le lire. Vous devez simplement vous assurer que votre collègue est l'unique et véritable destinataire de l'e-mail et lui garantir que vous en êtes bien l'expéditeur. La sécurité nationale n'est pas en jeu, mais si un concurrent de votre entreprise s'emparait de ce document, il pourrait beaucoup vous en coûter. Comment pouvez-vous procéder ? Vous pouvez recourir à la **cryptographie**. Peut-être aurez-vous le sentiment que l'aspect dramatique des phrases codées chuchotées dans de sombres couloirs fait défaut, mais le résultat est le même : les informations sont révélées uniquement aux personnes souhaitées.

1.1. Définition de la Cryptographie :

Lacryptographieest la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle nous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données, **la *cryptanalyse***est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalyses sont également appelés des **pirates**. La **cryptologie**englobe la cryptographie et la cryptanalyse.

La cryptographie répond aux besoins suivant:

- Gérer l'Authentification et contrôler les accès aux données (signature numérique, mots de passe)
- Permettre la confidentialité.
- Vérifier l'intégrité.)
- Assurer la non-répudiation.

1.2. Les outils de la cryptographie :[04]

Les outils cryptographiques utilisant le principe de clé pour sécuriser les liens de communication sont nombreux

a)Expéditeurs et destinataire :

Supposons qu'un expéditeur veux envoyer un message a un destinataire.Cet expéditeur veux envoyer le message de manière sure : il veut s'assurer qu'aucune oreille indiscrète ne puisse s'informer du message.

b) Message et chiffrement :

Un message est appelées texte en claire. Le processus de transformation d'un message de telle manière à le rendre incompréhensible est appelée chiffrement(ou encryptions).le résultat de ce processus de chiffrement est appelée texte chiffré(ou cryptogramme).Ces différents processus sont illustrées par la **figure 3** suivante :

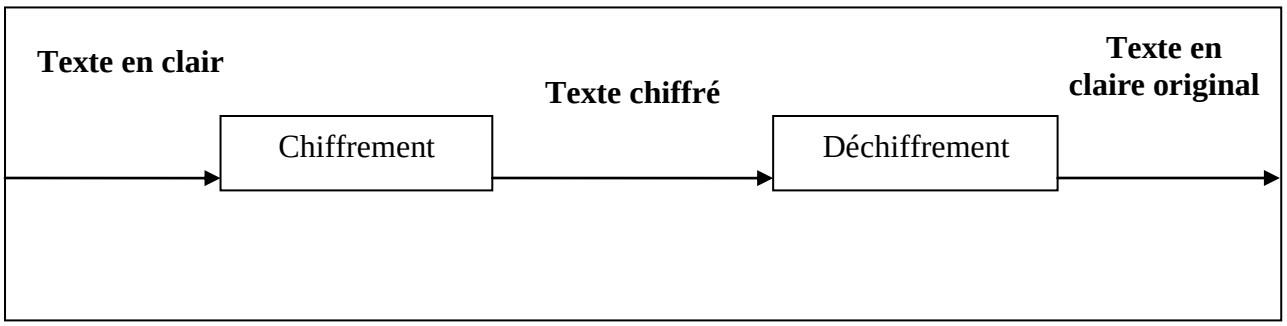


Figure 3 : Chiffrement –déchiffrement.

c) Notion de Clé: c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

2.2. Évolution de la cryptologie :[05]

2.1. Méthodes classique :

2.1.1. Système manuel :

a) Chiffrement de César :

L'un des premiers systèmes de chiffrement fut probablement celui utilisé par **JulesCésa**r il y a environ 2000 ans. Le principe appliqué consistait à remplacer chaque lettre de l'alphabet par celle située trois places plus loin dans l'ordre alphabétique. S'il fallait dépasser la lettre **Z**, on revenait à la lettre **A**. Ce système est un exemple de substitution car chaque lettre est toujours remplacée par une même lettre.

L'alphabet de substitution utilisé par le système de chiffrement de **César** est indiqué ci-dessous.

Alphabet : **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Substitution : **DEFGHIJKLMNOPQRSTUVWXYZABC**

Si l'on applique ce système, le texte **MA PETITE VACHE AMALAUX PATTES** devient **PD SHWLWH YDFKH D PDO DXA SDWWHV**, ce qui peut être représenté sous forme continue comme **PDSHWLWHYDFKHDPDODXASDWWHV** pour plus de confidentialité.

Dans certains cas, les lettres chiffrées peuvent être regroupées en blocs de 5 caractères. Si l'on procédait de la sorte, on obtiendrait : **PDSHW LWHYD FKHDP DODXA SDWWH V**.

Substitutions, permutations et transpositions.

Le système de chiffrement de César offre un exemple de substitution mono-alphabétique où les lettres sont remplacées de façon précise. Évidemment, il n'est pas nécessaire de remplacer toutes les lettres comme l'a fait César. Par exemple, on peut utiliser la table de substitution suivante :

Alphabet : **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Substitution : **QWERTYUIOPASDFGHJKLZXCVBNM**

Si on chiffrait le message **SOYEZ AUX AGUETS** avec cet alphabet, on obtiendrait le résultat suivant : **LGNTM QXB QUXTZL**.

- **Inconvénients :**

Ce système de cryptage est très simple à mettre en œuvre, cependant étant totalement symétrique, il suffit de faire une soustraction pour connaître le message initial. Une méthode primaire est d'essayer les 26 combinaisons possibles et voir si l'on peut obtenir un message compréhensible. Une méthode plus évoluée consiste à calculer les fréquences d'apparition des lettres dans le message codé (ce qui est beaucoup plus facile lorsque le message est long).

Effectivement, selon la langue, certaines lettres reviennent plus couramment que d'autres (en français, par exemple, la lettre la plus utilisée est la lettre E), ainsi la lettre apparaissant le plus souvent dans un texte crypté par le chiffrage de César correspondra vraisemblablement à la lettre E, une simple soustraction donne alors la clé de cryptage.

b) Méthode de Porta

Ce système fut mis au point en 1563 par l'Italien Giovanni Batista da Porta. Sa méthode est décrite au moyen de la table ci-dessous. Elle nécessite un **mot-clé**dont les lettres forment les **lettres-clés.**

La première colonne (contenant des paires de lettres en caractère gras) contient la composante du mot-clé. La rangée du haut, aussi indiquée en caractère gras, contient la composante primaire du texte en clair. Leur association permet une substitution réciproque pour une lettre-clé particulière.

Supposons une lettre-clé. Si la lettre du texte en clair figure dans la rangée du haut, on lui substitue la lettre qui apparaît à l'intersection de la colonne où se trouve la lettre en clair et de la rangée où se trouve la lettre-clé. Si la lettre du texte en clair n'est pas affichée dans la rangée du haut, on la cherche dans la rangée où se trouve la lettre-clé et on lui substitue la lettre correspondante.

	a	b	c	d	e	f	g	h	i	j	k	l	m
AB	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	r	s	t	u	v	w	x	y	z	n	o	p	q
UV	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	o	p	q	r	s	t	u	v	w	x	y	z	n

Tableau 1: Tableau de porta.

Chiffrons **BATAILLEDEMAINMATIN** en utilisant comme mot-clé le mot **SECRET**.

La première lettre-clé est **S** et donc la rangée qui nous concerne est :

	a	b	c	d	e	f	g	h	i	j	k	l	m
ST	r	s	t	u	v	w	x	y	z	n	o	p	q

La première lettre du texte en clair est **B** et donc la lettre chiffrée est **S**. La deuxième lettre clé est **E** et on regarde donc les deux rangées suivantes :

	a	b	c	d	e	f	g	h	i	j	k	l	m
EF	y	z	n	o	p	q	r	s	t	u	v	w	x

La deuxième lettre du texte en clair est **A** et donc la lettre chiffrée est **Y**. La troisième lettre clé est **C** et on isole les deux rangées suivantes :

	a	b	c	d	e	f	g	h	i	j	k	l	m
CD	z	n	o	p	q	r	s	t	u	v	w	x	y

La troisième lettre du texte en clair est **T** et il s'en suit que la lettre chiffrée est **H**. Le chiffrement complet donne lieu au texte chiffré suivant (en notant que les lettres du mot-clé sont répétées autant de fois que nécessaire) :

Mot clé : **SECRETSECRETSECRETS**

Texte en clair : **BATAILLEDEMAINMATIN**

Texte chiffré : **SYHSTPPPPWXRZCYSIZJ**

c) Méthode de Vigenère :

Cette méthode de chiffrement est le fruit du travail de Blaise de **Vigenère**, un Français ayant vécu de 1523 à 1596. Il semble qu'elle fut mise au point par **Vigenère** lors de ses visites au Vatican. Le principe à la base de cette méthode consiste à utiliser une différente substitution alphabétique à chaque position, ce qui rend l'analyse des fréquences un peu moins attrayante. Un mot- clé est utilisé et écrit à maintes reprises au haut du texte en clair tout comme dans la méthode de Porta.

Dans l'exemple qui suit, le mot-clé est **MONTREAL**. Pour chiffrer, on choisit la rangée de la table ci-dessous qui correspond à la lettre appropriée du mot-clé et on opère une substitution alphabétique avec la lettre située à l'intersection de la colonne correspondant à celle-ci et de la rangée correspondant à la lettre du texte en clair. Le chiffrement du texte en clair s'effectue donc par autant de substitutions différentes qu'il y a de lettres dans le mot-clé.

Mot clé : **MONTREALMONTREALMO**

Texte en clair : **CHARDASSAUTADROITE**

Texte chiffré : **OVNKUESDMIGTUVOTFS**

Pour cette méthode, le destinataire doit connaître le mot-clé et la table de chiffrement. Cette table peut être aussi simple que celle présentée ci-dessous. Le déchiffrement est accompli en procédant à l'inverse, tout simplement.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tableau 2: tableau de Vigenère

d) Méthode de Playfair :

Ce système fut inventé par Charles Wheatstone, un professeur de philosophie au King'sCollège de Londres, en Angleterre. Ce système reçut son nom en 1854 lorsque Lyon Playfair, baron de St. Andrews, présenta la méthode lors d'un banquet. Le chiffrement de Playfair fut utilisé par les Britanniques pendant la guerre des Boers et la Première Guerre mondiale.

Voici une version simplifiée de cette méthode de chiffrement :

Remplir une table de dimension 5 par 5 avec des lettres de l'alphabet en groupant deux des 26 lettres. Ceci peut être accompli avec un mot-clé en inscrivant consécutivement dans la table la première apparition de chaque lettre du mot-clé suivie des autres lettres de l'alphabet. La **table ci-dessous** est construite à partir du mot-clé **VANCOUVER** et en groupant **I** et **J**.

V	**A**	**N**	**C**	**O**
U	**E**	**R**	**B**	**D**
F	**G**	**H**	**I/J**	**K**
L	**M**	**P**	**Q**	**S**
T	**W**	**X**	**Y**	**Z**

Tableau 3 : Tableau de Playfair.

Écrire le texte en clair par groupes de deux lettres. Si une paire contient la même lettre deux fois, on ajoute une *lettre complémentaire* (comme le **X**) entre les deux.

Par exemple, **MISSION EN VIGUEUR** s'écrit comme suit **MI SX SI ON EN VIGU EU RX**.

La lettre complémentaire est **X** et est utilisée à deux occasions, la deuxième fois pour compléter la dernière paire du message.

Pour chaque paire de lettres, **la table 3** est utilisée comme suit :

Si les lettres sont dans la même colonne, chacune des deux est remplacée par la lettre située immédiatement en dessous; si une lettre est au bas de la colonne, elle est remplacée par celle se trouvant au haut de la colonne, si les lettres sont dans la même rangée, chacune est remplacée par la lettre située immédiatement à sa droite; si l'une des lettres est la dernière de la rangée, elle est remplacée par la première de la même rangée si les deux lettres ne se trouvent ni dans la même rangée, ni dans la même colonne, elles sont remplacées comme suit:

la première lettre chiffrée est obtenue en prenant la lettre située à l'intersection de la rangée contenant la première lettre du texte en clair et de la colonne comprenant la seconde lettre du texte en clair; la deuxième lettre chiffrée est obtenue en prenant l'intersection de la colonne contenant la première lettre du texte en clair et de la rangée contenant la deuxième lettre du texte en clair.

Les étapes du chiffrement du texte en clair de l'exemple ci-haut sont présentées dans le **tableau ci-dessous**. Le texte chiffré est ensuite écrit en une séquence continue de lettres : **QGPZQKVCRACFFEREHN**.

Texte en clair	Cas	Texte chiffré
MI	Diff rentes rang e et colonne	QG
SX	Diff rentes rang e et colonne	PZ
SI	Diff rentes rang e et colonne	QK
ON	M me rang e	VC
EN	Diff rentes rang e et colonne	RA
VI	Diff rentes rang e et colonne	CF
GU	Diff rentes rang e et colonne	FE
EU	M me rang e	RE
RX	M me colonne	HN

- **Inconvénients :**

De même que la méthode de César, même si elle est plus complexe, on peut aisément décrypter un message en étudiant les couples de lettres qui apparaissent le plus souvent dans le message chiffré, et en supposant qu'ils représentent les diagrammes les plus courants dans la langue (par exemple pour le français : *'es'*, *'en'*, *'on'*, *'ou'*, *'te'*, *'nt'*, et *'de').*

2.2.2. Systèmes mécaniques

Les systèmes manuels sont souvent lents et laborieux pour l'usager puisque fondés sur l'emploi de papier et crayons. De plus, ils ne permettent pas l'utilisation d'algorithmes compliqués. Des méthodes de chiffrement plus rigoureuses et complexes utilisant des appareils mécaniques ont donc été mises au point. La section qui suit offre un bref aperçu des plus célèbres de ces machines à chiffrer mécaniques.

a) Appareils à disques codeurs :

Le premier appareil à disque codeur fut inventé par Léon Battista Alberti au 15e siècle. Il était formé de deux disques concentriques en cuivre, l'un de ces disques étant grand et fixe, et l'autre plus petit et mobile. Ces disques étaient divisés en 24 parties radiales égales. Le disque extérieur contenait les lettres du texte en clair dans l'ordre suivant :

{ A,B,C,D,E,F,G,I,L,M,N,O,P,Q,R,S,T,V,X,Z,1,2,3,4 }, c'est-à-dire un nombre suffisant de lettres de l'alphabet pour former la majorité des mots latins. De plus, le disque intérieur contenait la permutation suivante de l'alphabet latin :

{m, r, d, l, g, a, z, e, n, b, o, s, f, c, h, t, y, q, i, x, k, v, p, et}.

Ce mécanisme, quoique assez simple en lui-même, illustre l'ingéniosité d'Alberti, qui combine pour la première fois une substitution dite poly-alphabétique et l'usage d'un code.

b) Le cylindre à roues codeuses M-94/CSP-488 :

En 1922, l'armée américaine fit fabriquer le M-94, un appareil cylindrique comportant 25 anneaux (de diamètre d'environ 4 cm) en aluminium sur un pivot d'environ 10,5 cm de long. Ce mécanisme demeura en service jusqu'au début de la Deuxième Guerre mondiale.

Il fut aussi utilisé par la garde côtière et la «Federal Communications Commission» desÉtats-Unis. La marine américaine avait une version semblable dans la CSP-488.

Figure 4 : Le cylindre à roues codeuses M-94/CSP-488

c) Le convertisseur M-209 de Hagelin :

Fabriqué par Boris Hagelin au début des années 1940 pour l'armée américaine, le M-209 était un appareil mécanique simple mesurant 18 cm de large par 14 cm de profond et 9 cm de haut.

Il pouvait être rangé dans un sac de toile vert et pesait environ 4 kilogrammes. Ses composantes principales incluaient six roues codeuses à 26, 25, 23, 21, 19 et 17 positions respectivement, assurant une longueur de cycle (c'est-à-dire le nombre d'étapes avant qu'une clé donnée se répète) de 101 405 850 pas. Pour manipuler cet appareil, l'utilisateur devait tourner le bouton externe (situé à gauche) afin de choisir la lettre du texte en clair, puis tourner ensuite la manivelle située à droite afin d'activer les composantes internes. Vers la fin de la révolution de cette manivelle, l'appareil imprimait la lettre chiffrée sur une bande-papier. Pendant la

Deuxième Guerre mondiale, plus de 140 000 unités de cet appareil furent fabriquées, principalement par la firme «Smith Corona Typewriter» aux États-Unis.

Figure 5 : Le convertisseur M-209 de Hagelin

2.2.3. Systèmes électromécaniques

Des machines à chiffrement assez complexes et efficaces fonctionnant notamment avec des piles comme source d'énergie furent mises au point au 20e siècle. Plusieurs furent utilisées pendant la Deuxième Guerre mondiale.

a) La machine Enigma :

Ayant pour origine des brevets de 1919 d'Alexandre Koch et des brevets d'Arthur Scherbius durant les années 1920, l'Enigma fut produite en version commerciale en 3 modèles : A, B et C. Le modèle C était un appareil qui n'avait pas d'imprimante, mais plutôt un mécanisme qui illuminait les lettres chiffrées. Tous les modèles possédaient un clavier. Pendant les années 1930, l'Allemagne se réarmait et fit l'acquisition de la compagnie Enigma. Une version à trois roues codeuses de l'Enigma fut jugée adéquate en termes de sécurité. Pendant la Deuxième Guerre mondiale, cette Enigma portative à lampes (de grandeur et de poids similaires à ceux d'une machine à écrire) alimentée par une pile et logée dans une boîte en chêne servit l'armée (*Armee)*, la marine (*Kriegsmarine*), et les forces aériennes (*Luftwaffe*) allemandes.

Figure 6: la machine Enigma

b) Les machines de Hebern :

En 1910, Edward H. Hebern commença à mettre au point des machines de chiffrement auxÉtats-Unis. Au début des années 1920, il inventa la machine à code électriquequi utilisait une seule roue codeuse. Il conçut aussi, en 1924, des appareils à trois et cinq roues codeuses comme prototypes pour la marine américaine. Très différentes d'enigma, les machines de Hebern utilisaient des roues codeuses dont le filage interne pouvait facilement être changé. De plus, ces roues codeuses pouvaient fonctionner dans le sens de rotation conventionnel ou dans le sens contraire. Par contre, ces machines possédaient toutes des faiblesses du point de vue Cryptanalytique.

c) Les machines TYPEX et SIGABA :

À la suite d'une longue étude (1926-1935) portant sur les machines de chiffrement commerciales commes les machines Hebern, Kryha et Enigma, un comité interministériel britannique adopta une machine semblable à l'Enigma appelée Typex. Le modèle Mark III de Typex avait cinq roues codeuses interchangeables dotées d'un mouvement irrégulier. Cet appareil électrique était lourd et imprimait le texte chiffré sur bande-papier, l'imprimante étant située à l'arrière de la machine. Plusieurs versions de la Typex furent utilisées par l'armée britannique et la RAF.

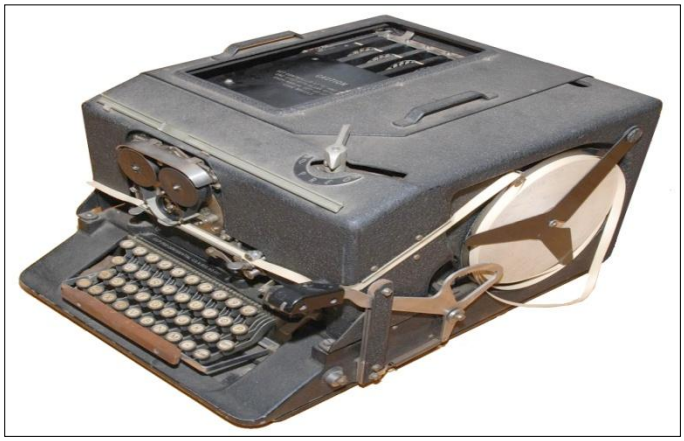


Figure 7 : La machine SIGABA

2.2. La cryptographie moderne :

De tous temps, les services secrets ont utilisé toutes sortes de codages et de moyens cryptographiques pour communiquer entre agents et gouvernements, de telle sorte que les "ennemis" ne puissent pas comprendre les informations échangées. La cryptologie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Ainsi, très peu de gens, voire personne n'utilisait la cryptographie à des fins personnelles. C'est pourquoi, pendant tant d'années, la cryptologie est restée une science discrète.

De nos jours en revanche, il y a de plus en plus d'informations qui doivent rester secrètes ou confidentielles. En effet, les informations échangées par les banques ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir les déduire.
C'est pourquoi ce genre d'informations est crypté. L'algorithme de cryptographie DES par exemple, est utilisé massivement par les banques pour garantir la sécurité et la confidentialité des données circulant sur les réseaux bancaires. Le système d'exploitation Unix, lui aussi, utilise ce procédé pour crypter ses mots de passe.

Finalement, la cryptologie est de plus en plus utilisée sur le réseau mondial internet. Avec l'apparition du commerce en ligne, c'est-à dire la possibilité de commander des produits directement sur internet, la cryptographie est devenue nécessaire. En effet, si les différents ordinateurs branchés sur internet sont sécurisés par des mots de passe, c'est-à-dire à priori inaccessibles par un ennemi, les transactions de données entre deux ordinateurs distants via internet sont, quant à elles, facile à intercepter. C'est pourquoi lorsque l'on commande un produit sur internet en payant avec notre carte bancaire, il est beaucoup plus sûr d'envoyer notre numéro de carte bancaire une fois crypté, celui-ci ne pourra à priori, être décrypté que par la société à laquelle on a commandé ce produit. C'est pour ces mêmes raisons d'insécurité sur Internet, et par un besoin humain d'intimité que la cryptographie à des fins purement personnelles s'est développée sur le réseau : pour la messagerie électronique. En effet lorsque l'on envoie un message électronique par internet, on peut préférer qu'il reste discret vis à vis de la communauté internet, voire qu'il ne soit compréhensible que par le destinataire du message. En d'autres termes, la cryptographie peut servir si l'on veut envoyer un message confidentiel, ou un message intime à quelqu'un. Cela est aujourd'hui possible grâce à la formidable distribution de logiciels gratuits permettant d'utiliser de la cryptographie "forte" très facilement. C'est le cas du logiciel PGP (Pretty Good Privacy = "assez bonne confidentialité") qui est distribué gratuitement sur internet, développé par Philip R. Zimmerman seul, en 1991. Ce sont pour toutes ces raisons que tout d'abord la cryptologie s'est énormément renforcée, et que finalement elle est passée d'un monde fermé comme les armées ou les services secrets à un monde ouvert à tout utilisateur.

2.1. Les méthodes de cryptographie moderne

1. Le chiffrement :

Le chiffrement est l'action de transformer une information claire, compréhensible de tout le monde, en une information chiffrée, incompréhensible. Le chiffrement est toujours associé au déchiffrement, l'action inverse. Pour ce faire, le chiffrement est opéré avec un algorithme à clé publique ou avec un algorithme à clé privée.

2. Les algorithmes à clé privé ou à clé secrète

a) Algorithme a clé privée

Les algorithmes à clé privée sont aussi appelés algorithmes symétriques. En effet, lorsque l'on crypte une information à l'aide d'un algorithme symétrique avec une clé secrète, le

destinataire utilisera la même clé secrète pour décrypter. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, par courrier, par téléphone ou lors d'un entretien privé.

.

b) Les algorithmes à clé publique

En effet, les algorithmes à clé publique sont aussi appelés algorithmes asymétriques. C'est à dire que pour crypter un message, on utilise la clé publique (connue de tous) du destinataire, qui sera à priori le seul à pouvoir le décrypter à l'aide de sa clé privée (connue de lui seul).

c) L'algorithme DES

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée **code produit.**

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k à k_{16}. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 2 (soit $7.2*10^{16}$) clés différentes.

d) L'algorithme RSA

L'algorithme RSA (du nom de ses inventeurs Ron Rivest, Adi Shamir et Len Aldeman, qui ont imaginé le principe en 1978) est utilisé pour la cryptographie à clé publique et est basé sur le fait qu'il est facile de multiplier deux grands nombres premiers mais difficile de factoriser le produit. C'est l'exemple le plus courant de cryptographie asymétrique, toujours considéré comme sûr, avec la technologie actuelle, pour des clés suffisamment grosses (1024, 2048 voire 4096 bits).

e) L'algorithme AES :

Aussi connu sous le nom de Rijndael lancé en 1997 ; Algorithme de chiffrement/déchiffrement symétrique (clef secrète).

Une même clef secrète est utilisée pour les opérations de chiffrement et de déchiffrement (c'est un secret partagé entre l'expéditeur et le destinataire du message).

AES est un algorithme de chiffrement par blocs, les données sont traitées par blocs de 128 bits pour le texte clair et le chiffré. La clef secrète a une longueur de 128 bits, d'où le nom de version : AES 128 (il existe deux autres variantes dont la clef fait respectivement 192 et 256 bits)

2.3 Conclusion :

Dans ce chapitre nous avons présenté l'historique de la cryptographie devisé en deux parties classiques et modernes.

Avec le développement technologique, protéger ses données est devenu une nécessité pour cela des systèmes de chiffrements ont été mis au point.

3.1 Introduction :

Les systèmes de chiffrements font appel à des algorithmes de chiffrements souvent complexes qui modifient, à l'aide d'une clé de chiffrement plus ou moins longue, les caractères à protéger pour générer des données aléatoires. Ils se composent de deux principales classes : symétrique et asymétrique.

3.2. Cryptographie symétrique : [06]

Par cryptographie symétrique, on fait référence à la cryptographie à clef secrète, les mécanismes de chiffrement et de déchiffrement utilisant la même clef pour les deux interlocuteurs Alice et Bob. Au sein de ce domaine, on distingue plusieurs familles de primitives qui permettent de répondre à différents besoins. Premièrement, on trouve les algorithmes de chiffrement qui permettent de transformer un message en clair en un message chiffré pour en assurer la confidentialité. On dispose ensuite de fonctions de hachage, qui sont utilisées dans beaucoup de domaines de la cryptographie et permettent par exemple de construire une empreinte d'un message pour en attester une certaine l'intégrité. Enfin, pour garantir l'authenticité de l'origine d'un message, on peut utiliser les codes d'authentification de message (MAC).

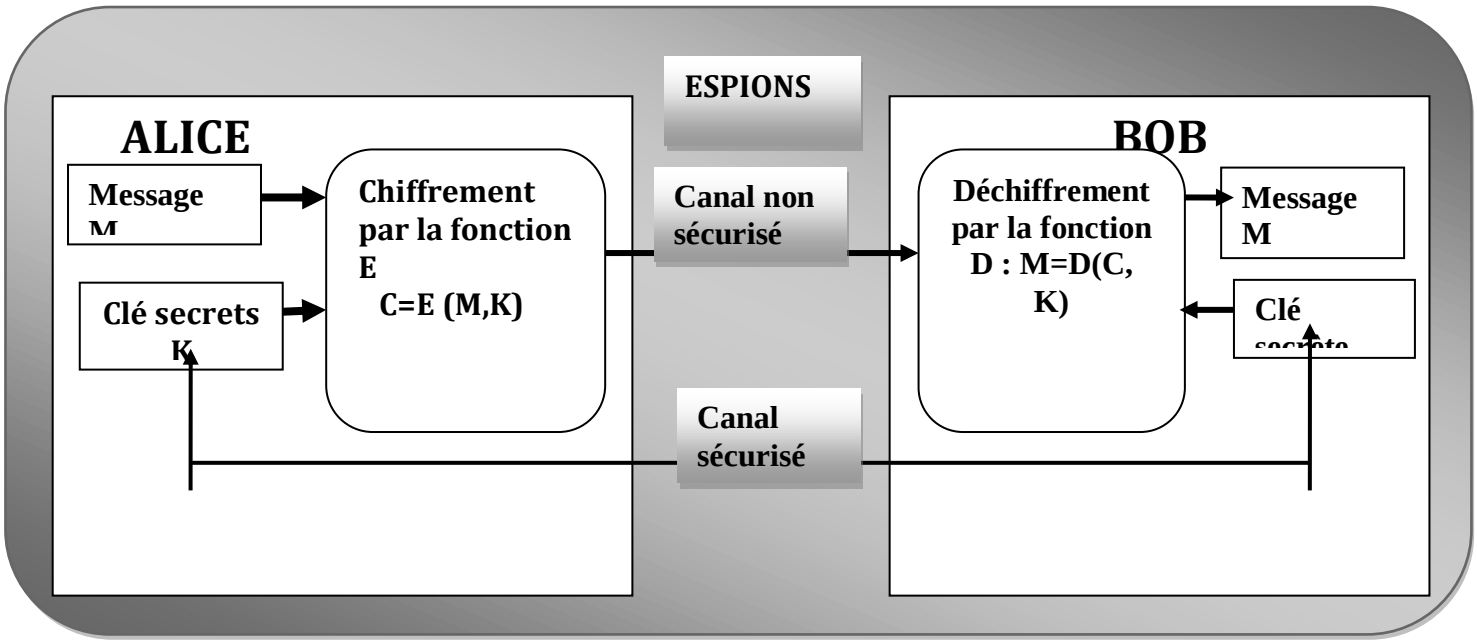


Figure 8 : schéma crypto- système symétrique

2.1. Algorithmes de chiffrement par bloc

Cette primitive de chiffrement est la plus répandue et consiste en un algorithme déterministe paramétré par une clef et qui travaille sur un groupe de bits de taille fixe appelé **bloc**. Pour chiffrer (ou déchiffrer) un message de longueur arbitraire, on utilise un mode opératoire qui permet de lier les résultats de chiffrements des blocs successifs et ainsi produire le chiffrement du message complet. En 1977, le National Bureau of Standards (désormais le National Institute of Standards and Technology, NIST) annonce le **DES** comme standard de chiffrement **[DES]** : il s'agit d'un algorithme initialement développé par IBM qui utilise le réseau de Horst Feistel. Vingt ans plus tard, et après de nombreuses attaques publiées sur le DES, le NIST lance le concours AES (Advanced Encryptions Standard) qui sélectionne un nouveau standard de chiffrement en 2000 **AES01**. Complètement différent de son prédécesseur le DES, ce sont les cryptographes belges Joan Daemen et Vincent Rijmen qui remportent le concours avec leur soumission Rijndael, parmi les 15 autres algorithmes proposés.

a) Algorithme Data Encryption Standard (DES):

Le DES est l'un des algorithmes de cryptage les plus utilisés dans le monde, pendant de nombreuses années et auprès de nombreuses personnes, secret de l'information et DES furent synonymes.

Avant d'entrer dans les détails, faisons d'abord un petit voyage dans le temps afin de connaitre les conditions et les raisons qui ont mené a la naissance de l'incroyable algorithme DES.

Publié le 06 aout 1977 par le NBS (National Bureau of Standards), le DES est un algorithme de chiffrement de données recommandé pour les organisations à caractère fédéral, commercial ou privé. Le DES tire son origine des travaux menés par le groupe cryptographique d'IBM dans le cadre du projet LUCIFER. Le DES a été l'objet de nombreuses implémentations, à la fois en matériel et en logiciel, depuis sa publication. Après une décennie de succès, pendant laquelle les moyens et techniques de cryptanalyse mis en œuvre pour en étudier les caractéristiques n'ont pas permis d'en découvrir des faiblesses inacceptables, le DES a, depuis peu, révélé des sensibilités à des attaques nouvelles et puissantes, parfois réalisées sur un simple micro-ordinateur. Aussi l'ISO (International Organization for Standardization) a-t-il récemment refusé la normalisation du DES, ce qui n'empêche pas cet algorithme d'être, de loin, aujourd'hui encore comme le moyen de chiffrement le plus sûr (et le plus largement utilisé) pour des données non militaires.

Le DES est un algorithme de chiffrement symétrique par blocs qui permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits (56 bits servant à chiffrer + 8 bits de parité servant à vérifier l'intégrité de la clef en réalité).

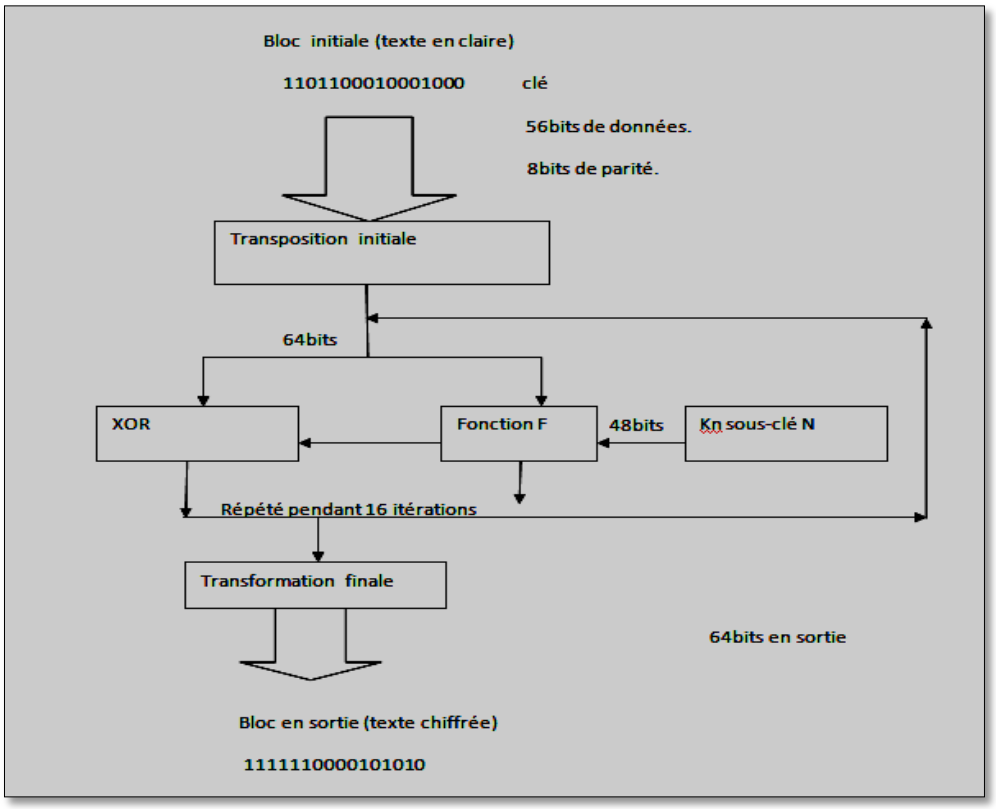


Figure 9: Schéma général de l'algorithme DES

Voici les différentes étapes de l'algorithme du DES :

- **Fractionnement du message:**

Dans un premier temps le message en clair est découpé en blocs de 64 bits.

- **Transposition initiale :**

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Chaque bit d'un bloc subit une permutation selon l'arrangement du tableau c'est-à-dire que le 58ème bit du bloc se retrouve en 1ère position, le 50ème en seconde position,etc…

- **Scindement en bloc de 32 bits:**

Le bloc de 64 bits est scindé en deux blocs de 32 bits notés G et D. On notera G0 et D0 l'état initial de ces deux blocs.

G0

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

D 0

57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

On remarque que G0 contient tous les bits pairs du message initial et D0 tous les bits impairs.

- **Rondes**

Les blocs Gi et Di sont soumis à un ensemble de transformation appelée rondes. Une ronde est elle-même composée de plusieurs étapes :

- **Fonction d'expansion :**

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Les 32 bits du bloc D0 sont étendus à 48 bits grâce à une table d'expansion dans laquelle 32 bits sont mélangés et 16 d'entre eux sont dupliqués. Ainsi, le 32ème bit devient le premier, le premier devient le second… Les bits 1,4,5,8,9,12,13,16,17,22,21,24,25,28,29 et 32 sont dupliqués et disséminés pour former un bloc de 48 bits que l'on nommera D'0 .

- **OU exclusif (XOR) avec la clef :**

DES procède ensuite à un OU exclusif entre D'0 et la première clef k1 générée à partir de la clef K (que doivent se partager émetteur et destinataire) par l'algorithme de cadencement des clefs que nous décrirons plus bas. Nous appellerons D''0 le résultat de cette opération.

- **Boîtes de substitution :**

D''0 est découpée ensuite en 8 blocs de 6 bits, noté D'0i . Chacun de ces blocs passe par des boîtes de substitution(S-boxes), notées généralement Si. Les premier et dernier bits de chaque D0i déterminent la ligne de la fonction de substitution, les autres bits déterminent la colonne. Grâce à cela la fonction de substitution « choisit » une valeur codée sur 4 bits (de 0 à 15). Voici la première boîte de substitution :

S1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Soit D0i égal à 010101, les premiers et derniers bits donnent 01, c'est-à-dire 1 en binaire. Les bits autres bits donnent 1010, soit 10 en binaire. Le résultat de la fonction de substitution est donc la valeur située à la ligne n°1, dans la colonne n°10. Il s'agit de la valeur 6, soit 0110 en binaire. Chacun des 8 blocs de 6 bits est passé dans la boîte de substitution correspondante. Voici les autres S-Boxes :

S2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	5	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

On obtient donc en sortie 8 blocs de 4 bits. Ces bits sont regroupés pour former un bloc de 32 bits.

- **Permutation :**

Le bloc de 32 bits subit une permutation dont voici la table :

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

- **OU exclusif :**

Le bloc de 32 bits ainsi obtenu est soumis à un OU exclusif avec le G0 de départ pour donner D1 et le D0 initial donne G1. L'ensemble de ces étapes est itérée seize fois.

- **Transposition initiale inverse:**

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Au bout des seize itérations, les deux blocs G16 et D16 sont « recollés » pour reformer un seul bloc de 64 bits puis subit la transposition initiale inverse selon l'arrangement du tableau. On obtient alors le bloc initial chiffré.

- **Reconstruction du message chiffré**

Tous les blocs sont collés bout à bout pour obtenir le message chiffré.

- **Algorithme de cadencement des clefs**

Nous allons décrire l'algorithme qui permet de générer à partir d'une clef de 64 bits, 8 clefs diversifiées de 48 bits chacune servant dans l'algorithme du DES. De prime abord les clefs de

parité sont éliminées pour obtenir une clef de 56 bits. Ce bloc subit une permutation puis est découpée en deux pour obtenir 2 blocs de 28 bits décrits par les matrices ci-dessous :

40	8	48	16	56	24	64	40	8	48	16	56	24	64
39	7	47	15	55	23	63	39	7	47	15	55	23	63
38	6	46	14	54	22	62	38	6	46	14	54	22	62
37	5	45	13	53	21	61	37	5	45	13	53	21	61

Ces deux blocs subissent une rotation à gauche, c'est-à-dire que les bits en seconde position prennent la première position, ceux en troisième position la seconde, celle en première position la dernière…

14	17	11	24	1	5	3	28	15	6	21	10
13	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	57	45
44	49	39	56	34	53	46	42	50	36	29	32

Les 2 blocs sont regroupés pour faire un bloc de 56 bits qui passe par une permutation fournissant un bloc de 48 bits représentant la clef ki. :

Des itérations de l'algorithme permettent de donner les 16 clefs utilisées dans l'algorithme du DES.

b) Algorithme Advanced Encryption Standard (AES)

Les principes des codes symétriques commerciaux modernes du type **DES** (Data Encryptions Standard) ont été mis au point dans les années 1970 par IBM avec l'aide de la NSA (National Security Agency), ce sont des hybrides de codes de substitutions et de codes de transpositions. Ils restent très surs avec des clés assez courtes de 128 bits à 256 bits. Leur sûreté est non prouvée. Leur cryptanalyse a fait des progrès (cryptanalyse linéaire et différentielle), ce qui permet de mieux cerner leur sûreté. Les codes à clé secrète sont les plus employés actuellement car ils sont éprouvés, résistants, rapides et assez facile `a mettre en œuvre. Actuellement leur sécurité est garantie (mais non prouvée) avec des clés assez courtes de 128 à 256 bits pour le standard actuel AES.

- **Présentation générale de l'algorithme AES**

L'**AES** (Advanced Encryption Standard) est, comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le **DES** (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles. Historiquement, le développement de l'AES a été instigué par le **NIST** (National Institue of Standards and Technology).
Il est également approuvé par la **NSA** (National Security Agency) pour l'encryptions des informations dites très sensibles.

Cet algorithme suit les spécifications suivantes :

- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.
- C'est un algorithme de type symétrique.
- C'est un algorithme de chiffrement par blocs.
- Il supporte différentes combinaisons **[longueur declé]-[longueur de bloc]: 128-128**, **192-128** et **256-128** bits (en fait, l'AES supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard)

En termes décimaux, ces différentes tailles possibles signifient concrètement que:

3.4 x 1038 clefs de 128-bit possibles
6.2 x 1057 clefs de 192-bit possibles
1.1 x 1077 clefs de 256-bit possibles

Pour avoir un ordre d'idée, les clés **DES** ont une longueur de 56 bits (64 bits au total dont 8 pour les contrôles de parité), ce qui signifie qu'il y a approximativement 7.2 x 1016 clés différentes possibles. Cela nous donne un ordre de 1021 fois plus de clés **128** bits pour l'AES que de clés **56** bits pour le **DES**. En supposant que l'on puisse construire une machine qui pourrait cracker une clé **DES** en une seconde (donc qui puisse calculer 255 clés par seconde), alors cela prendrait environ 149 mille milliards d'années pour cracker une clé AES.

- **Le principe de fonctionnement de l'AES :**

AES : est une méthode de chiffrement par blocs de 128, 192 et de 256 bits [74]. Chaque bloc est transformé en une matrice de 16 (4x4) octets à quoi on applique les opérations suivantes pour atteindre un texte chiffré à partir du texte en clair (figure 3 .3) :

  - **Sub_Byte** : substitution de chaque élément du texte en clair.
  - **Shift_Rows** : décalage des lignes en fonction de leurs numéros.

- **Mix_Columns** : multiplication de chaque colonne par un polynôme pour obtenir une transformation linéaire.
- **Add_Round_Key :** application de l'opérateur mathématique XOR entre la matrice transformé et une sous partie de la clé.

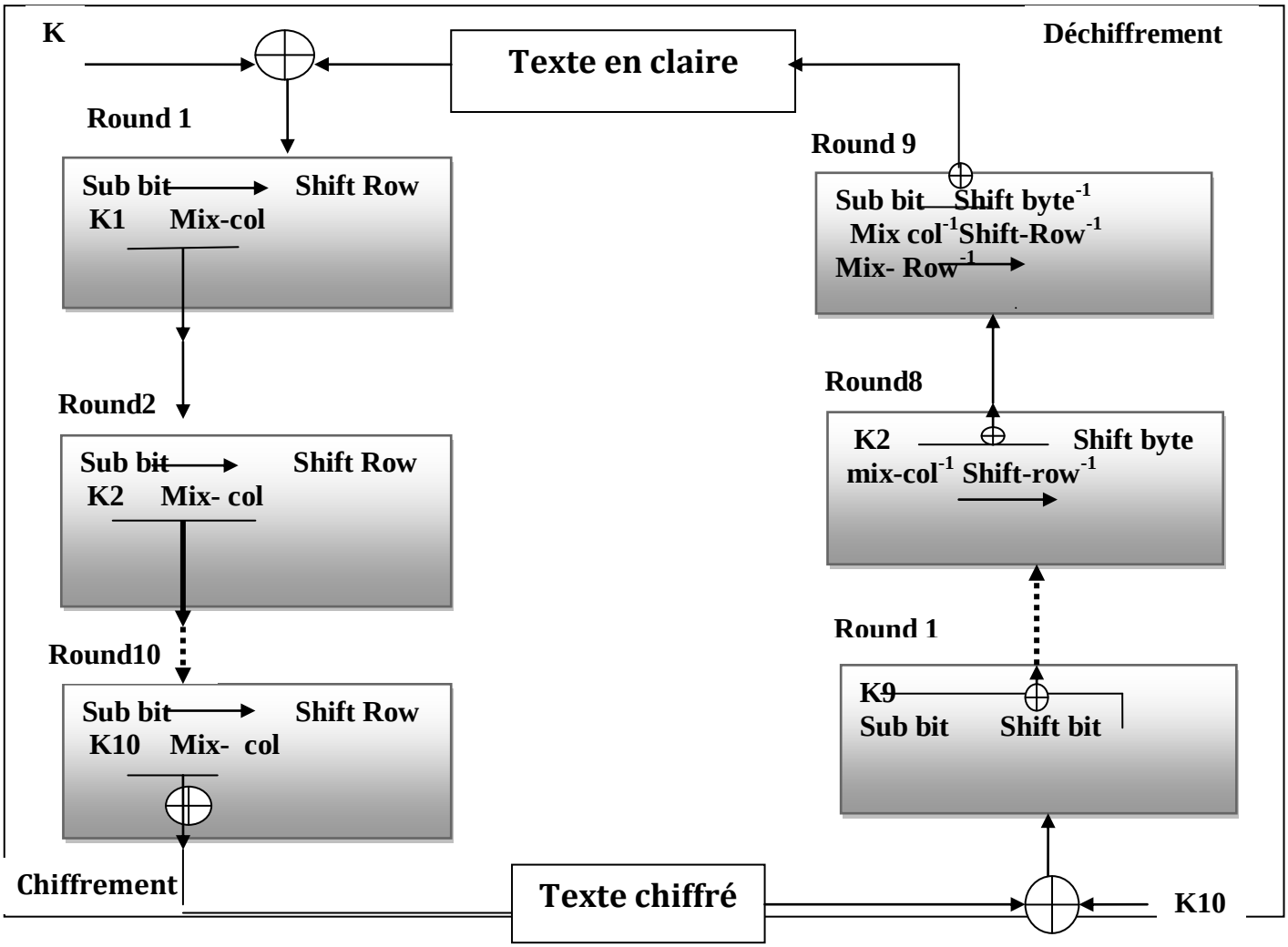


Figure 10 : Schéma général de l'algorithme AES

2.3. Caractéristiques et points forts de l'AES :

Le choix de cet algorithme répond à de nombreux critères plus généraux dont nous pouvons citer les suivants :

- Sécurité ou la résistance nécessaire pour une éventuelle cryptanalyse.
- Puissance de calcul qui entraine une grande rapidité de traitement.
- Besoins en ressources et mémoire très faibles.

- Flexibilité d'implémentation, cela inclut une grande variété de plateformes et d'applications ainsi que des tailles de clés et de blocs supplémentaires.
- Compatibilité hardware et software, il est possible d'implémenter l'**AES** aussi bien sous forme logicielle que matérielle.
- Simplicité : le design de l'AES est relativement simple.
- Si l'on se réfère à ces critères, on constate que l'**AES** est également un candidat particulièrement approprié pour les implémentations embarquées qui suivent des règles beaucoup plus strictes en matière de ressources, puissance de calcul, taille mémoire, etc. C'est sans doute cela qui a poussé le monde de la **3G (3ème génération de mobiles)** à adopter cet algorithme pour son schéma d'authentification.

3.3. Cryptographie asymétrique:

En 1976 , whiffieddiffied et martin Helleman introduisent la cryptographie a clé publique .Un crypto-système asymétrique utilise deux clés différentes pour les opérations de chiffrement et déchiffrement : une clé publique et une clé privée ; la clé privée doit obligatoirement rester secrète, quant a la publique, elle est connu par tous les algorithmes a clé publique sont très performants en matière de sécurité, mais présentent l'inconvénient d'être très lents.

Dans la pratique, on ne chiffre pas une donnée entière avec un algorithme asymétrique, mais on chiffre une empreinte de la donnée en question. Cette empreinte est obtenue grâce à une fonction de hachage.

Dans cette partie, nous nous proposons d'étudier un algorithme de chiffrement asymétrique très utilisée qui est le **RSA,** ainsi qu'une fonction de hachage qui est la **MD5.**

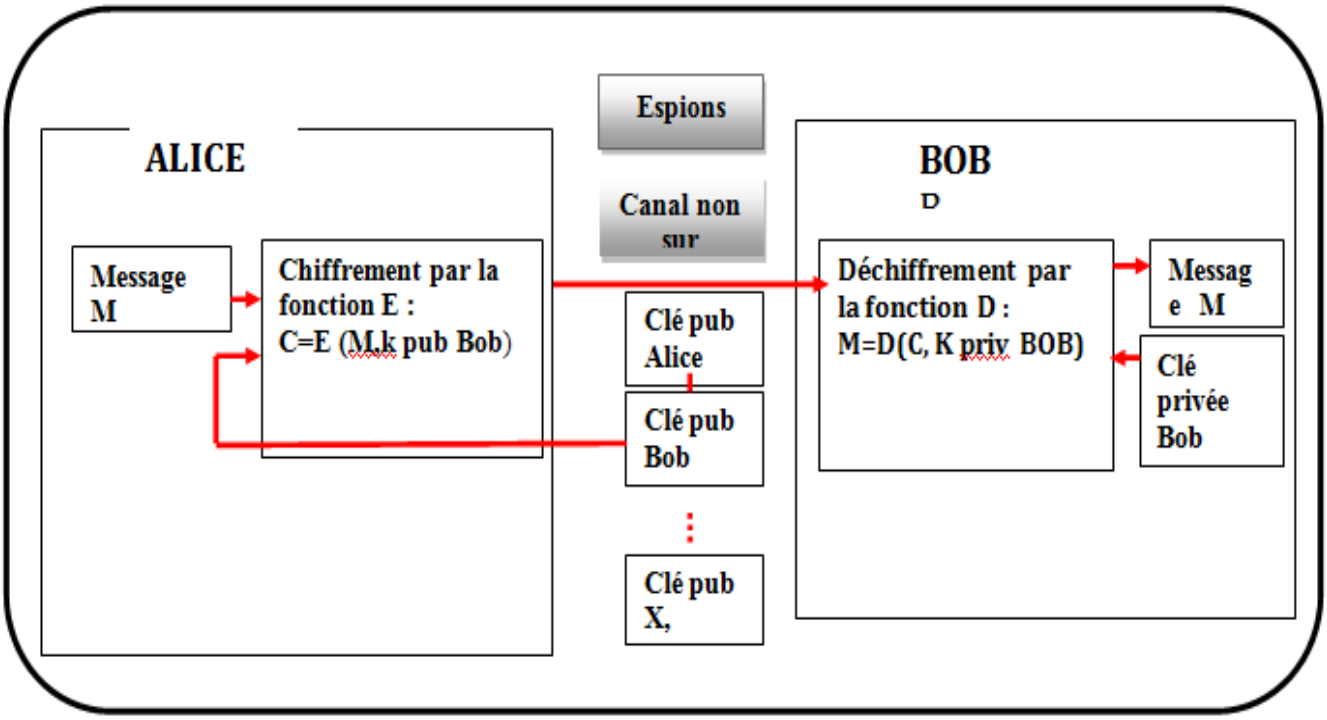


Figure 11 : Crypto-système asymétrique

a) L'algorithme Rivest-Shamir-Adleman(RSA) :

Inventé en 1977 par Ron Rivest, Adi Shamir et Len Adelman, le système de cryptage RSA est un système à clé publique qui devint rapidement une référence.

- **Initialisation** :

❖ Choisir deux nombres premiers, p et q, les deux étant plus grands que 10100.

❖ Calculer n = p · q (n est le *modulus*)

❖ Choisir e aléatoire tel que e et ((p - 1) * (q - 1)) n'aient aucun facteur commun excepté 1.

Trouver d tel que (e * d) soit divisible par ((p - 1) · (q - 1)), donc : ed = 1 mod ((p - 1)(q - 1)).

Clé publique : valeurs (n,e).

Clé privée : valeurs (n,d) = (p,q,d)

- **Chiffrement/Déchiffrement :**

L'expéditeur crée le texte chiffré c à partir du message m :

$c = m^e \bmod(n)$, où (n,e) est la clé publique du destinataire

Le destinataire reçoit **c** et effectue le déchiffrement : m = cd mod (n), où (n,d) est la clé privée du destinataire

- **Signature numérique :**

L'expéditeur crée la signature s à partir du message m :
s = md mod(n), où (n,d) est la clé privée de l'expéditeur.

Le destinataire reçoit s et m et effectue la vérification de m : m = s*e mod (n), où (n,e) est la clé publique de l'expéditeur.À titre de comparaison, le RSA est 1500 fois plus lent que le DES, du fait de sa complexité

- **Génération des clés** :
  - la base de RSA est le nombre n .ce nombre doit être le produit de 2 nombre premiers p et q très grand et ayant sensiblement le même nombre de chiffre.
  - Une fois n est calculé, on Alice cherche a déterminer la fonction d'Euler Q associée a n avec la formule : Q(n)=(p-1)*(q-1).
  - Une fois calcule, elle lui faudra de choisir sa clé publique **e, avec** e compris entre 2 et n et premier relativement a Q.

- A génère deux grands nombres premiers **p** et qpar des algorithmes probabilistes.
- A calcule (n = p * q) et φ (n) = φ (p, q) = (p-1) (q-1) et détermine e tel que e ^ φ (n) = 1, c'est-à-dire PGCD (e, φ(n)) = 1.
- A détermine d tel que ed ≡ 1 mod (φ(n)).
-A envoi le couple (e, n) à B. (e, n) est la clé publique de A.
- Le couple (d, n) est la clé privée de A.
- B chiffre son message M en utilisant la clé publique (e, n) de A et obtient le message chiffré C calculé comme suit : C = Me mod n, et le transmet à A.
- A déchiffre le message C et obtient le message original en exécutant l'opération suivante : M = Cd mod n.

L'atout majeur de RSA est le niveau de sécurité élevé qu'il garantit car il est facile pour deux communicants A et B de créer un grand nombre premier à partir du produit de deux autres nombres premiers et il est difficile, pour des nombres premiers assez grands, à un attaquant de retrouver la factorisation en deux nombres premiers pour le grand nombre premier généré. Ses inconvénients majeurs sont son temps de calcul important et la taille de ses clés (au minimum 1024 bits).

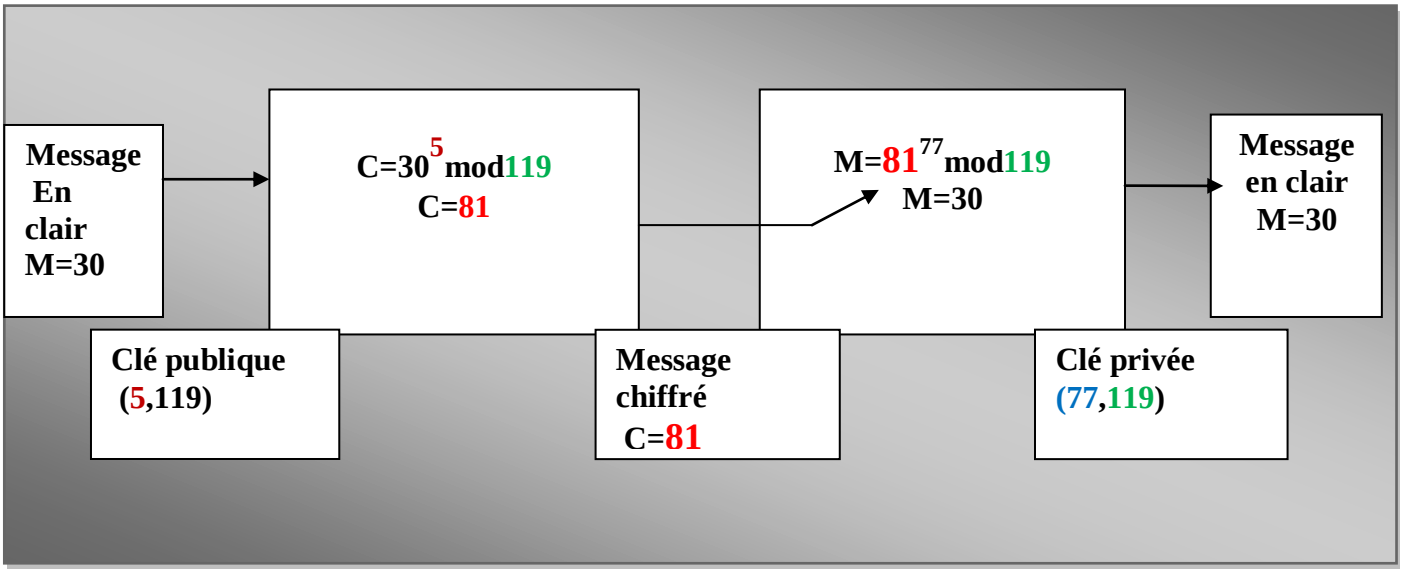


Figure 12: Exemple de déroulement de l'algorithme RSA

RSA est un algorithme de cryptage très performant, mais il ne faut pas oublier que cette puissance repose avant tout sur la difficulté de factoriser de grands entiers .Aujourdhui, il apparait indispensable de chiffrer avec des clés assez longues :au moins 1024 bits pour bien protégé .il faut toutefois noter que ,depuis un certains temps, les recherches menées sur le factorisation des grands nombres donnent de bonne résultats notamment grâce a deux mathématiciens néerlandais H.W et A.K .Lestera.

3.4. La fonction de hachage MD5 : [07]

L'algorithme**MD5**, pour **Message Digest 5**, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message). Il a été inventé par Ronald Rivest en 1991.L'utilisation de cette fonction de hachage dans les signatures numériques peut conduire à de multiples scénarios d'attaque et n'est plus considérée comme un composant fiable de l'infrastructure à clés publiques. Cependant dans le calcul de la « signature » d'un fichier il reste plutôt fiable, même si l'on ne peut pas assurer qu'il y a unicité entre l'empreinte calculée et le fichier ou message source.

1. Historique :

MD5 (Message Digest *5*) est une fonction de hachage cryptographique qui calcule, à partir d'un fichier numérique, son **empreinte numérique**(en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que deux fichiers différents donnent deux empreintes différentes.

En 1991, Ronald Rivest améliore l'architecture de MD4 pour contrer des attaques potentielles qui seront confirmées plus tard par les travaux de Hans Dobbertin.

Cinq ans plus tard, en 1996, une faille qualifiée de « grave » (possibilité de créer des collisions à la demande) est découverte et indique que MD5 devrait être mis de côté au profit de fonctions plus robustes comme SHA-1.

En 2004, une équipe chinoise découvre des collisions complètes. MD5 n'est donc plus considéré comme sûr au sens cryptographique. On suggère maintenant d'utiliser plutôt des algorithmes tels que SHA-256, RIPEMD-160 ou Whirlpool.

Cependant, la fonction MD5 reste encore largement utilisée comme outil de vérification lors des téléchargements et l'utilisateur peut valider l'intégrité de la version téléchargée grâce à l'empreinte. Ceci peut se faire avec un programme comme ***md5sum*** pour MD5 **et *sha1sum*** pour SHA-1.

Comme toute fonction de hachage cryptographique, MD5 peut aussi être utilisé pour calculer l'empreinte d'un mot de passe avec la présence d'un ***sel***permettant de ralentir une attaque par force brute. Cela a été le système employé dans GNU/Linux. Ainsi, plutôt que de stocker les mots de passe dans un fichier, ce sont leurs empreintes MD5 qui sont enregistrées, de sorte que quelqu'un qui lirait ce fichier ne pourrait pas découvrir les mots de passe. La commande **enable secret** des commutateurs et routeurs Cisco, utilisait le hachage MD5 pour stocker le mot de passe du mode privilégié dans le fichier de configuration de l'équipement. Les dernières versions d'IOS intègrent le hachage SHA256.

Le programme John the ripper permet de casser (trouver une collision pour) les MD5 triviaux par force brute. Il est incommode pour les clés longues, et ne fonctionne pas toujours si elles contiennent des caractères nationaux spécifiques (cela dépend en fait des dictionnaires utilisé).

2 .La somme de contrôle :

Très concrètement, la vérification de l'empreinte ou somme de contrôle MD5 peut être réalisée de la façon suivante : lors du téléchargement d'un programme, on note la série de caractères nommée « Signature MD5 » indiquée sur la page de téléchargement. Quand ce téléchargement est terminé, on lance un utilitaire de calcul MD5 comme, par exemple : **HashCalc ou md5sums,** qui indique entre autres la somme de contrôle correspondant au

fichier. Si les deux valeurs correspondent, on peut alors raisonnablement considérer que le fichier n'a pas été corrompu (volontairement ou non d'ailleurs). On constate plusieurs fragilités dans ce processus : la page d'origine a pu être modifiée, et l'utilitaire de calcul peut être adapté pour fournir la signature attendue. C'est pourquoi il faut impérativement utiliser un utilitaire provenant d'une source de confiance. Il est aussi possible d'utiliser une extension pour le navigateur Mozilla Firefox comme **MD Hash tool**[4] afin d'automatiser ce contrôle.

MD5 est donc un algorithme rapide et simple a implémenté et plutôt fiable. **MD5**va nous permettre de signer des ficher et de nous assurer qu'une transmission de donnée sans faille ni compromission.

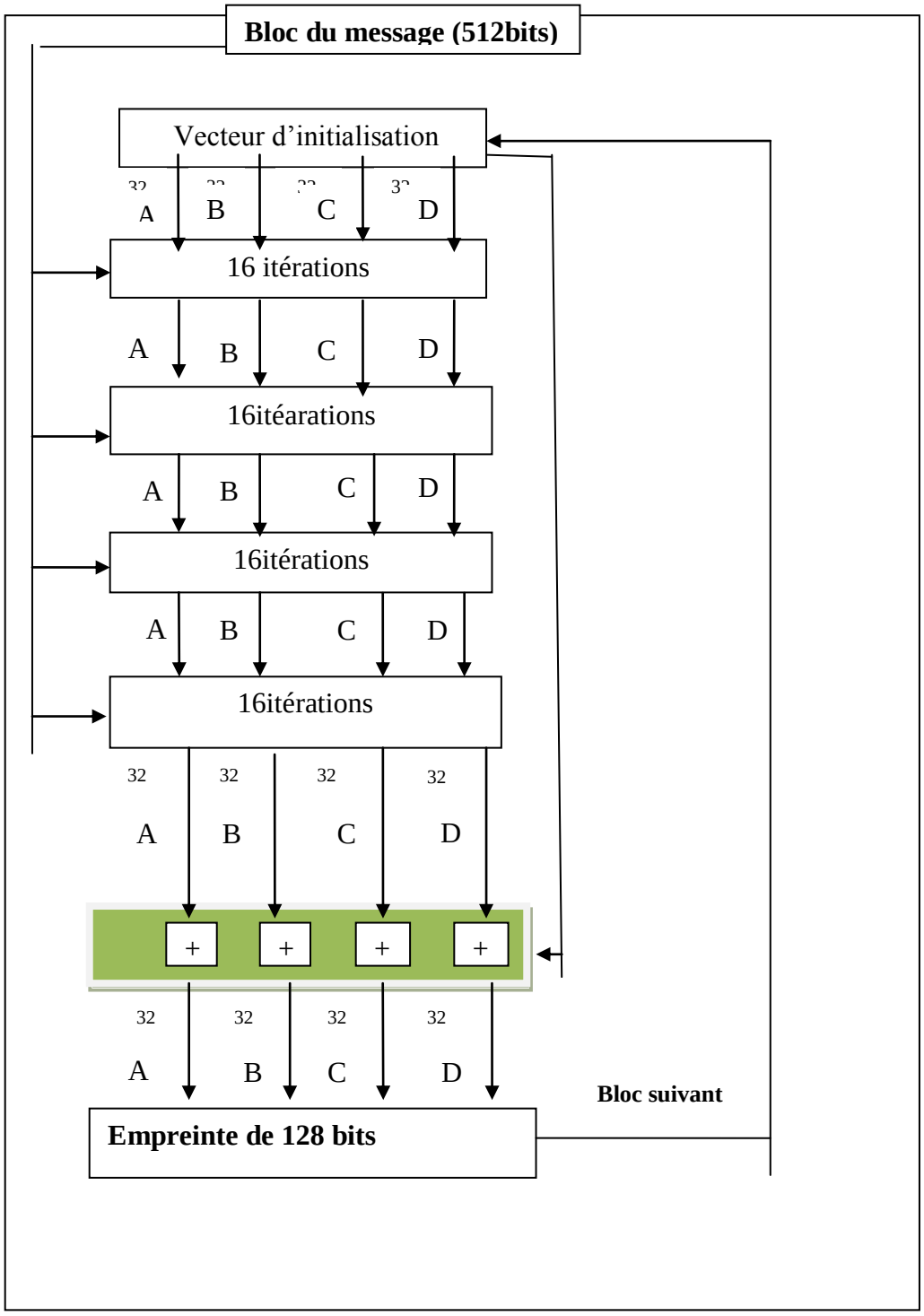


Figure 13: Vue générale de MD5

3.5. Comparaison des chiffrements symétrique et asymétrique :

Les deux parties que nous venons de voir illustrent deux types d'algorithmes de chiffrement : les algorithmes symétriques (a clé secrète)et asymétriques (a clé publique).On peut alors se demander les avantages et inconvénients qu'aurait un crypto système utilisant l'un ou l'autre des deux types d'algorithmes cités ci –dessus.

5.1. Les avantages de la cryptographie symétrique:

- Calcul non couteux et rapide des clés.
- Les clés sont relativement courtes(en moyenne 128bits).
- Facilité d'implantation sur le hardware.

5.2.Les inconvénients de la cryptographie symetrique :

- La distribution de clés entre les entités communicantes est très problématique.
- Le nombre de clés à gérer accroit sensiblement avec le nombre de nœuds déployés.

5.3. Les avantages de la cryptographie asymétrique :

- Efficace contre la capture des nœuds.
- Facilité de la distribution des clés signature facile des messages.
- Nombre réduit de clés à distribuer.

5.4.Les inconvénients de la cryptographie asymétrique :

- Taille des clés.
- Trop lente.
- Gourmande en ressources physiques et énergétiques.
- Vulnérable aux attaques de type déni de service où un attaquant inonde le réseau avec des certificats numériques illégales obligeant les nœuds à calculer des clés publiques jusqu'à épuisement de leur énergie.

3.6. Cryptographie symétrique Vs Cryptographie asymétrique ?

Dans les systèmes basés sur la cryptographie symétrique, les faiblesses des nœuds capteurs sont contournées par la réduction des opérations de calculs et de stockage de clés. Contrairement aux systèmes symétriques, la cryptographie asymétrique nécessite des temps de calcul importants et une consommation d'énergie énorme due au calcul des algorithmes à

clés publiques et à la transmission des certificats numériques utilisés par le destinataire pour authentifier la clé publique reçue. Cependant, la gestion de clé dans les systèmes à clé privée (symétriques) est beaucoup plus compliqué à cause des difficultés rencontrées lors de la distribution, l'échange et la découverte des clés entre nœuds voisins. Un problème que résout le système à clés publiques par l'introduction de certificats numériques pour une seule paire de clés (privée / publique) par nœud utilisée dans le chiffrement et le déchiffrement des messages.

Bien que le chiffrement à clé publique possède de gros avantages, il demeure inapproprié pour les réseaux des capteurs sans fils pour sa lenteur d'exécution et son cout considérable en termes de ressources physiques et énergétiques. Cependant et malgré que le chiffrement à clé privée possède des inconvénients liés au problème de l'établissement de clés entre les nœuds, il demeure le système le plus approprié pour les réseaux de capteur sans fil.

3.7. Machine Enigma : [08]

En 1939, peu avant la seconde Guerre Mondiale, le Capitaine Baudoin, un français, fait présenter son ouvrage marquant la transition entre la cryptologie classique et la cryptologie moderne. Durant la Seconde Guerre Mondiale, la cryptographie connût un développement considérable notamment avec l'utilisation de la machine ENIGMA.

7.1. Historique :

Breveté en 1918 et vendues dès 1923 par l'ingénieur allemand Arthur Scherbuis,la premier machine électromécanique Enigma s'avère un échec commercial. La marine de guerre allemande s'y intéressé néanmoins et confie son évolution du chiffre du ministère de la guerre. Le modèle Enigma M3 est agrée et utilisée par la flotte allemande a partir de 1926 ; mais les messages codées envoyés par Enigma sont partiellement déchiffré des 1936 grâce au travail conjoint des services alliée du contre espionnage et d'un groupe de cryptanalystes polonais. Avec la machine électromécanique construite par Turing est appelée « bombe », il est en effet possible de déterminer le message-clef de six lettres (changer quotidiennement) ayant servis a crypter le message .Hélas, début 1942, une nouvelle machine Enigma M4 fait son apparition. Plus sophistiqué, elle exige 11mois à l'équipe scientifique dirigée par Alan Turing pour décoder ses messages.

C'est au total de 18000 messages émanant des machines Enigma qui sont décrypté durant la seconde guerre mondiale.

7.2. Les différente machines :

Il faut savoir que lorsqu'on parle de la machine Enigma, en réalité, on parle d'un ensemble de machines parfois très différentes entre elles sur le plan cryptographique.

Chaque armée disposait d'une version particulière d'Enigma. Les plus célèbres d'entre elles sont les machines de type M3 et M4 dont se servait la marine allemande, à cause de leur implication dans la Bataille de l'Atlantique et l'impact de leur décryptement sur la Seconde guerre mondiale. Mais qu'existe-il comme machines autres que M3 ou M4, et en quoi différaient-elles ? Toutes les variantes d'Enigma possèdent des rotors assemblés en un brouilleur comme pièce électromécanique servant de base au cryptage. Ce sont les caractéristiques de ce brouilleur qui différencient les machines entre elles, ainsi que l'adjonction ou non d'un tableau de fiches. La complexité du cryptage effectué par la machine augmente avec ces différents dispositifs. Nous reviendrons sur leur fonctionnement prochainement.

- **La machine Enigma standard:** Il s'agit de la machine employée par les armées de terre et de l'air allemandes, qui était la plus courante .Elle était dans son fonctionnement presque identique à la machine Enigma D vendue dans le commerce. Trois rotors étaient alignés dans le brouilleur.
- **La machine Enigma M3 :** La marine allemande, employait cette machine à partir de 1933. Elle était sensiblement plus difficile à décrypter que la machine standard, car bien qu'elle dispose du même nombre de rotors alignés simultanément dans le brouilleur, ceux-ci étaient choisi parmi un lot plus grand, proposant deux rotors en plus des trois initiaux.
- **La machine Enigma M4 :** Cette machine remplaça la machine Enigma M3 en 1942 dans les sous-marins et dans les stations sur la côte, et était beaucoup plus complexe d'un point de vue cryptographique : quatre rotors étaient alignés simultanément dans le brouilleur de celle-ci, les trois premiers étant choisis parmi un lot de huit rotors, et le dernier étant choisi parmi deux autres.
- **La machine Enigma G** : elle était utilisée par les services secrets allemands. Il s'agit également d'une version à quatre rotors, mais démunie d'un tableau de fiches. La rotation des rotors a été choisie rapide, ce qui était perçu comme un difficulté supplémentaire pour d'éventuels cryptanalystes. Mais il s'avère que cette particularité a ajouté une faille supplémentaire à la machine, une aubaine pour les décrypteurs de Bletchley Park.

7.3. Le fonctionnement d'Enigma :

- **Vue globale de la machine :**

La machine Enigma reproduit un chiffrage par substitution poly-alphabétique rendu complexe pour éviter tout décryptement. Nous allons procéder à l'explication du système électo-mécanique d'un Enigma standard, Dans ce modèle, elle se compose de trois éléments reliés par des câbles électriques :

- ✓ Un clavier pour entrer le texte clair.
- ✓ Un dispositif de cryptagequi remplace chaque lettre du texte clair par une lettre chiffrée.
- ✓ Un tableau lumineux qui affiche la lettre chiffrée.

Ainsi, lorsqu'on appuie sur une touche du clavier, un courant électrique issu du clavier traverse le dispositif de cryptage et allume une diode du tableau lumineux qui correspond à une lettre chiffrée.

- **Le dispositif de cryptage**

Le dispositif de cryptage se compose de deux éléments distincts, qui tour à tour vont substituer la lettre provenant du clavier par une autre. Un premier remplacement est effectué au niveau du tableau de fiches et une seconde au niveau du brouilleur.

Le tableau de fiches permet de remplacer une lettre par une autre. Concrètement, il existe des fiches, c'est-à dire des fils électriques, qui permettent de permuter le circuit d'un fil avec celui d'un autre. A titre d'indication, les clefs du jour de l'armée demandaient de brancher dix fiches, ce qui entraînait la permutation de 20 lettres, chiffre qui était constant, mais dans d'autres utilisations, moins de fiches pouvaient être utilisées

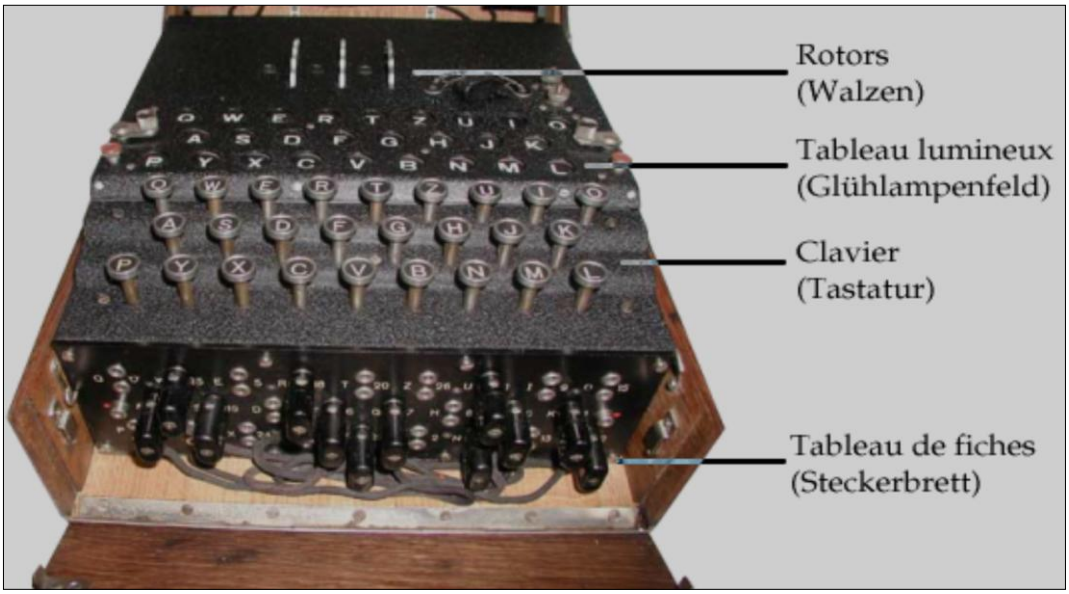


Figure 14: Les composants d'une machine Enigma standard.

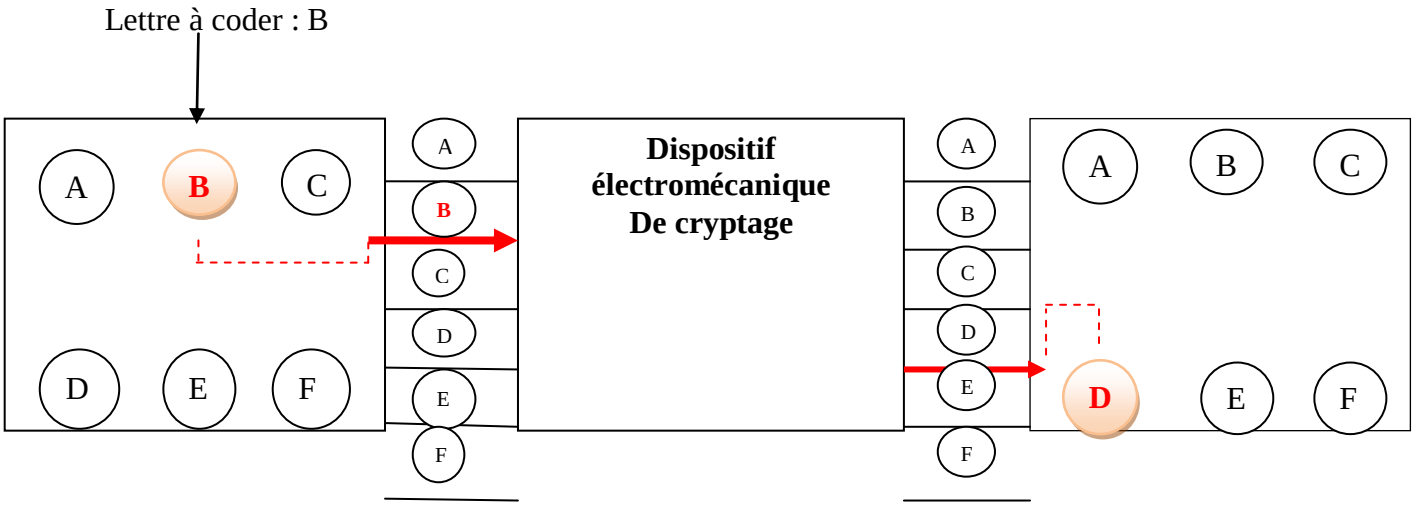


Figure 15 : Remplacement de B par D

Le codage d'un message avec Enigma se fait lettre à lettre : on entre la lettre sur un clavier et la machine indique la lettre codée correspondante sur un tableau lumineux. Exemple avec une machine disposant d'un alphabet de six lettres.

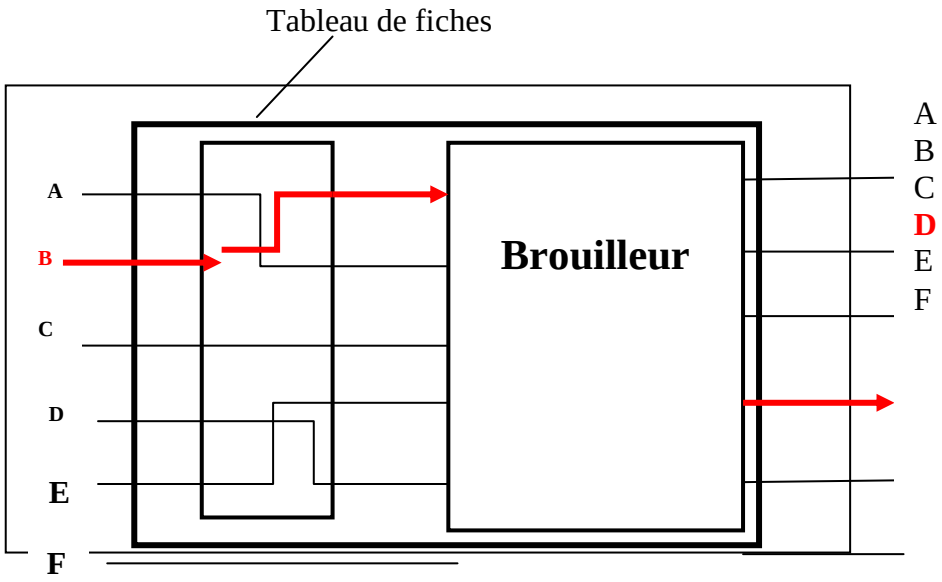


Figure 16 : Dispositif électromécanique de cryptage

Le dispositif de cryptage de la machine Enigma, composé du tableau de fiches et du brouilleur.

1) Le brouilleur

C'est l'élément essentiel du dispositif de cryptage. Dans une Enigma standard, il se compose de trois rotors et d'un réflecteur

2) Le rotor :

Un rotor est un disque composé d'un matériau isolant, de la taille d'un palet de hockey, et qui peut tourner selon un axe. Un rotor est pourvu de vingt-six contacts électriques sur chaque face. Les contacts de l'une des faces sont reliés aléatoirement aux contacts de l'autre face par des fils électriques qui passent à l'intérieur du corps du rotor. Ainsi si chaque contact correspond à une lettre, un rotor correspond à un alphabet codé. Une impulsion électrique qui arrive au rotor par le contact d'entrée représentant une lettre claire, par exemple A, émergera du rotor par le contact de sortie représentant une lettre chiffrée, par exemple C. Un rotor effectue donc une substitution mono-alphabétique, attribuant à chaque lettre claire une lettre chiffrée.

Enfin, le rotor est muni d'une bague non solidaire des câblages interne des rotors, sur laquelle des lettres sont gravées pour permettre à l'opérateur de repérer l'orientation du rotor

lorsqu'il règle sa machine. Si cette bague n'est pas solidaire des câblages, c'est pour ajouter à la complexité du cryptage d'Enigma. La bague devra être réglée au préalable sur la bonne position, mais ce système ne rend pas ce cryptage beaucoup plus fort, c'est pourquoi l'on n'entrera pas dans les détails.

L'un des principaux rôles du rotor est de tourner autour de son axe. Lorsque le rotor tourne, la correspondance entre circuit d'entrée et circuits de sortie est modifiée. Si le circuit A est relié au circuit C via le rotor, une fois que celui-ci ait tourné d'un cran, les connexions sont décalées d'un cran et donc le circuit A n'est plus relié au circuit C mais à un autre circuit, F par exemple. Un rotor peut pivoter vingt-six fois sur lui-même avant de retrouver sa position initiale.

3) Le réflecteur :

A ce stade des explications, on sait crypter une lettre à l'aide de la machine, mais l'on ne peut, à partir de la lettre chiffrée, retrouver la lettre originale. Il existe un dernier élément à la machine permettant de résoudre ce problème : le réflecteur. Grâce à lui, le chiffrement et le déchiffrement sont "symétriques", c'est à dire si F est codé B alors pour une même position des rotors,B est codé F.

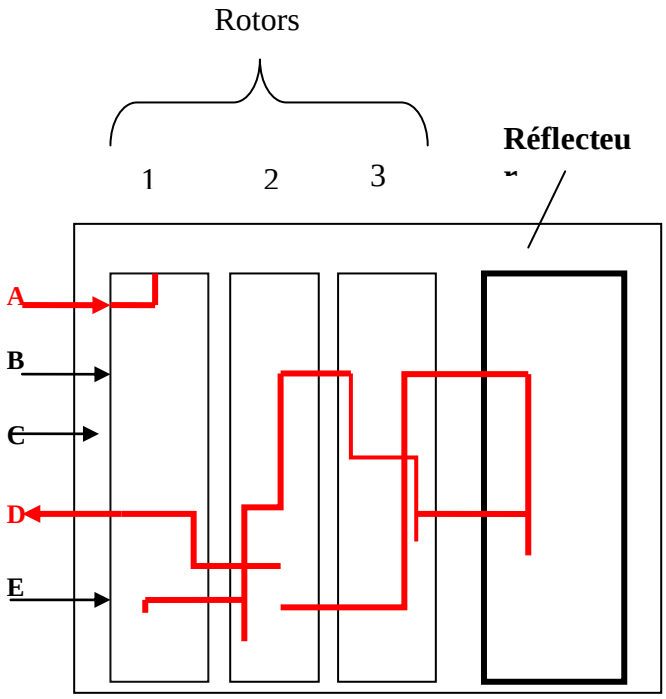


Figure 17: Les détails du brouilleur : trois rotors et un réflecteur

Le réflecteur fait partie du brouilleur et est situé après les trois rotors. Lorsqu'on enfonce une touche du clavier, un courant électrique qui lui est issu traverse le tableau de

fiches puis les trois rotors, le rôle du réflecteur est de renvoyer l'impulsion électrique en sens inverse dans les trois rotors puis de nouveau dans le tableau de fiches, avant qu'elle n'arrive au tableau lumineux pour afficher la lettre correspondante — cryptée ou décryptée (**Figure17).**

Cependant, le réflecteur a également généré une faiblesse de la machine Enigma largement exploitée plus tard par les cryptanalyses alliés : une lettre ne peut pas être codée par elle-même.

7.4. L'intérêt d'Enigma :

C'est à la nature dispersive des ondes radio que la machine Enigma doit sa participation à la guerre mondiale. Elle occupa la place centrale dans la sécurisation des communications allemandes en permettant de crypter les messages de nombreuses unités avant qu'ils ne soient envoyés. Elle multiplie les points forts : Rapide, la machine était plus simple à utiliser que d'autres procédés de cryptages puisqu'elle faisait intervenir un dispositif électromécanique automatique pour le cryptage, et évitait donc aux opérateurs l'effort qu'aurait nécessité un cryptage se faisant avec crayon et papier. Petite, elle était transportée aisément, ce qui augmentait le nombre de situations où elle pouvait se rendre utile, et permettait aussi de ne pas encombrer la mobilité des unités, point clef de la stratégie de la Blitzkrieg. Enfin, les Allemands ont pu établir un réseau très vaste de postes de TSF équipés de machines Enigma, puisqu'ils en étaient équipés de 30 000 au début de la guerre, pour un total de 200 000 machines construites à la fin de la guerre.

Pour les Allemands, la machine Enigma était tout ce dont l'armée avait besoin, en ce qui concernait la confidentialité de ses communications, pour la mise en œuvre de la Blitzkrieg. L'Allemagne nazie a eu une confiance aveugle en cette machine pour sécuriser les communications de toutes leurs armées et de certains des services en pensant que la machine était telle que l'avait vanté son concepteur Arthur Scherbius : imbattable.

4.1. Introduction :

Dans ce chapitre, nous allons présenter dans un premier lieu l'environnement de travail ainsi que les outils utilisés. En second lieu, nous allons présenter quelque capture d'écran de l'interface graphique de notre application.

Pour la mise au point de notre application nous nous somme inspiré du fonctionnement de la machine Enigma.

4.1. Environnement de développement:

Durant la réalisation de notre application, nous avant utilisé une machine ayant les caractéristiques suivantes :

- Un microprocesseur toshibacore^{tm} i5-2520M
- Fréquence d'horloge : 2.50/3.20 turbo GHz
- Disque dur 320Go

4.2. IDE (Interface DevelopementEnvironement) :

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin. En plus de Java, NetBeans permet également de supporter différents autres langages, comme Python, C, C++, JavaScript, XML, Ruby, PHP et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web).

Conçu en Java, NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Development Kit JDK est requis pour les développements en Java.

Logo	
Développeur :	Oracle
Première version :	1996, sous le nom de Xelfi1
Dernière version :	8.0.2(15.07.2015)
Environnements :	Multilingue
Type :	IDE pour Java, PhP, C/C++, Fortran, JavaScript, Python, Ruby
Licence :	CDDL/ GPL
Site web :	netbeans.org

4.3. Présentation des interfaces de notre application :

Nous allons présenter les différentes interfaces de l'application

a) Interface d'accueil :

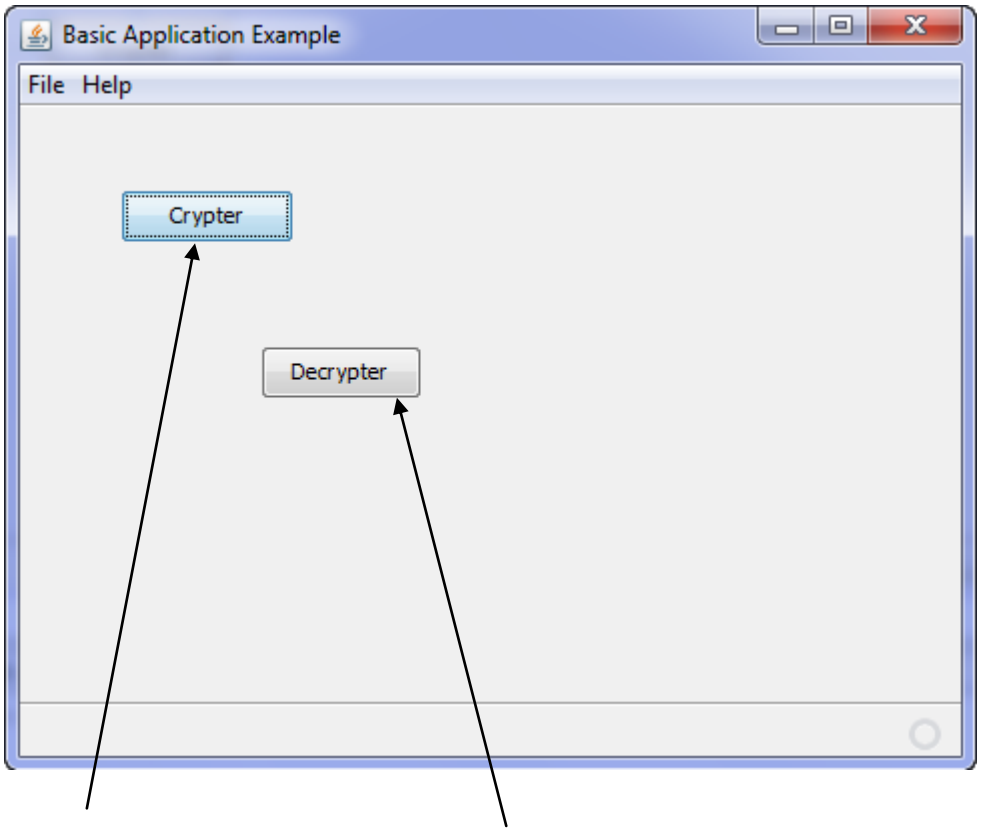


Figure 18: interface d'accueil

- **Bouton de « Cryptage »** : permet a l'utilisateur de lancer l'opération de cryptage.
- **Bouton de « Décryptage »** : permet de lancer l'opération de décryptage.

b) intérface de cryptage :

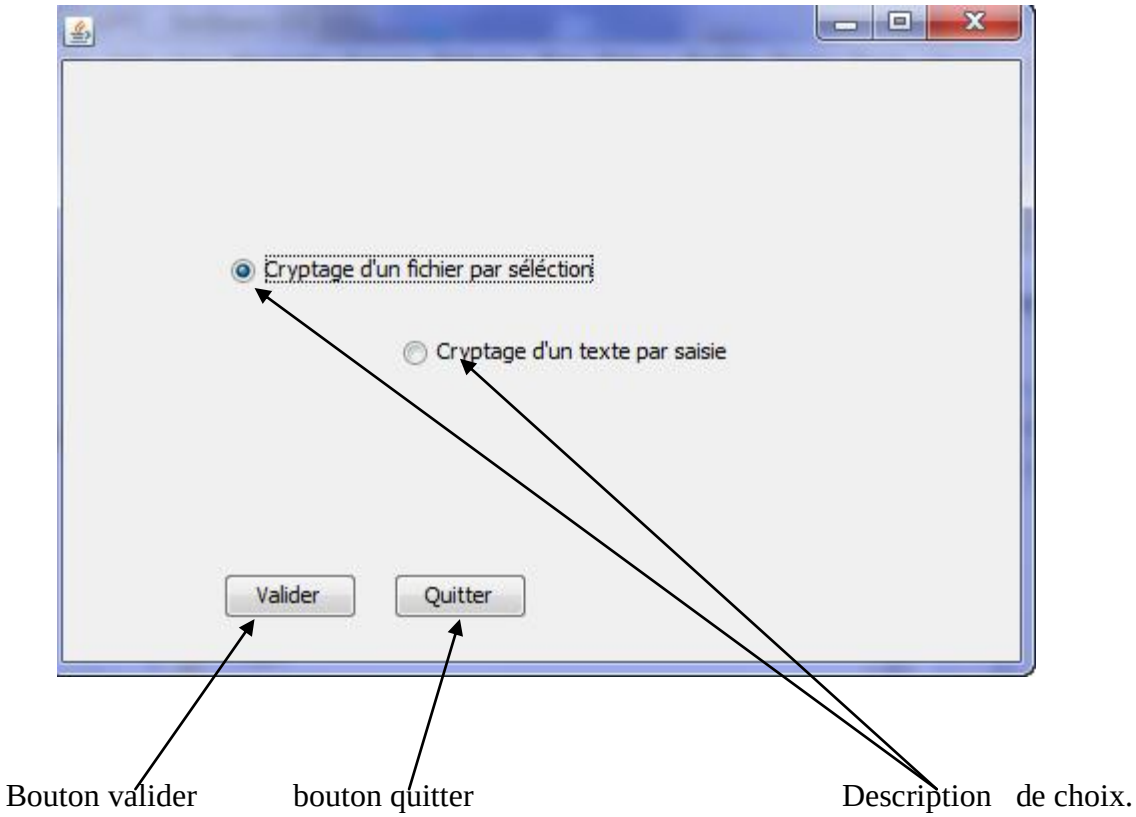
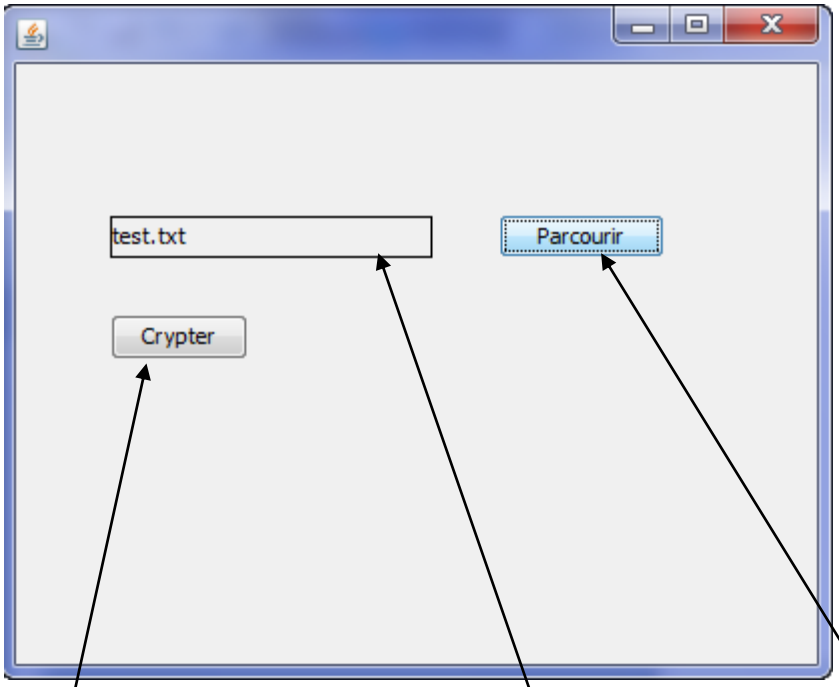


Figure 19: interface de cryptage

Description de choix : l'utilisateur choisi de crypter par sélection de fichier, ou bien par saisi de texte.

- **Bouton « valider »:** permet de valider le choix de l'utilisateur.
- **Bouton « quitter »:** permet de quitter la fenêtre de choix.

c) Fenêtre de sélection de fichier a crypté :



Bouton de cryptage le fichier a crypté bouton parcourir

Figure 20: interface de cryptage de fichier

L'utilisateur sélectionne le fichier à crypter en cliquant sur le bouton parcourir qui lui permet de choisir un fichier dans un répertoire. La figure représente l'interface procréée par ce bouton.

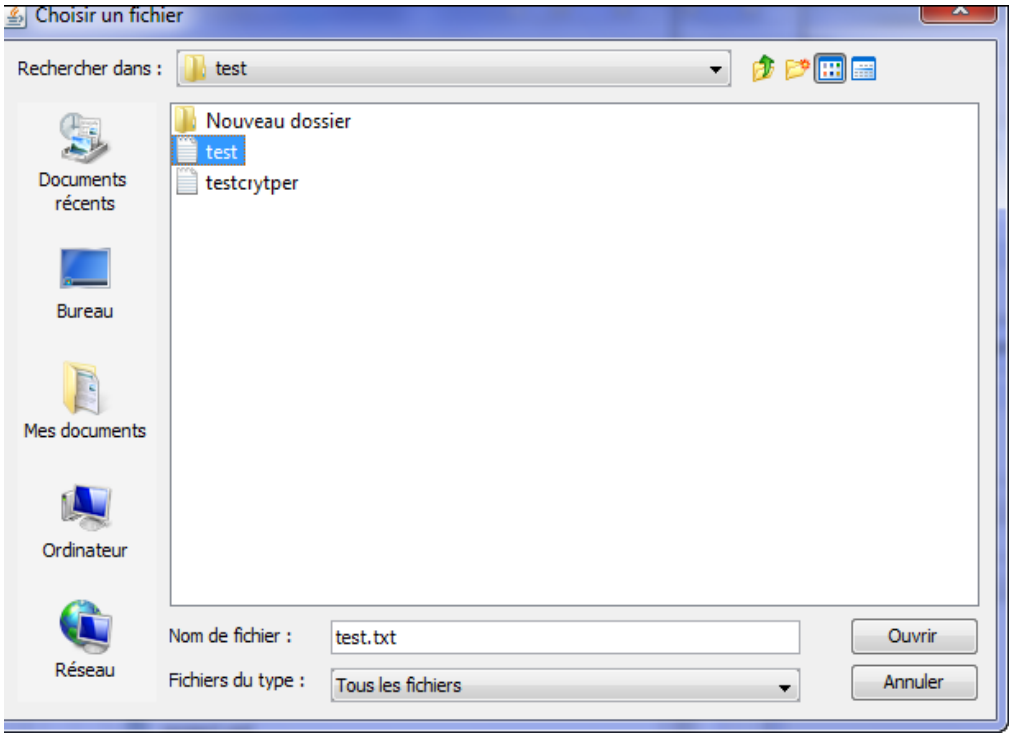


Figure 21: interface pour choisir le fichier à crypter

Après avoir sélectionné le fichier qu'on veut crypter, il faut cliquer sur le bouton « crypter » qui fait appel a l'algorithme de cryptage.

d) Cryptage par saisie :

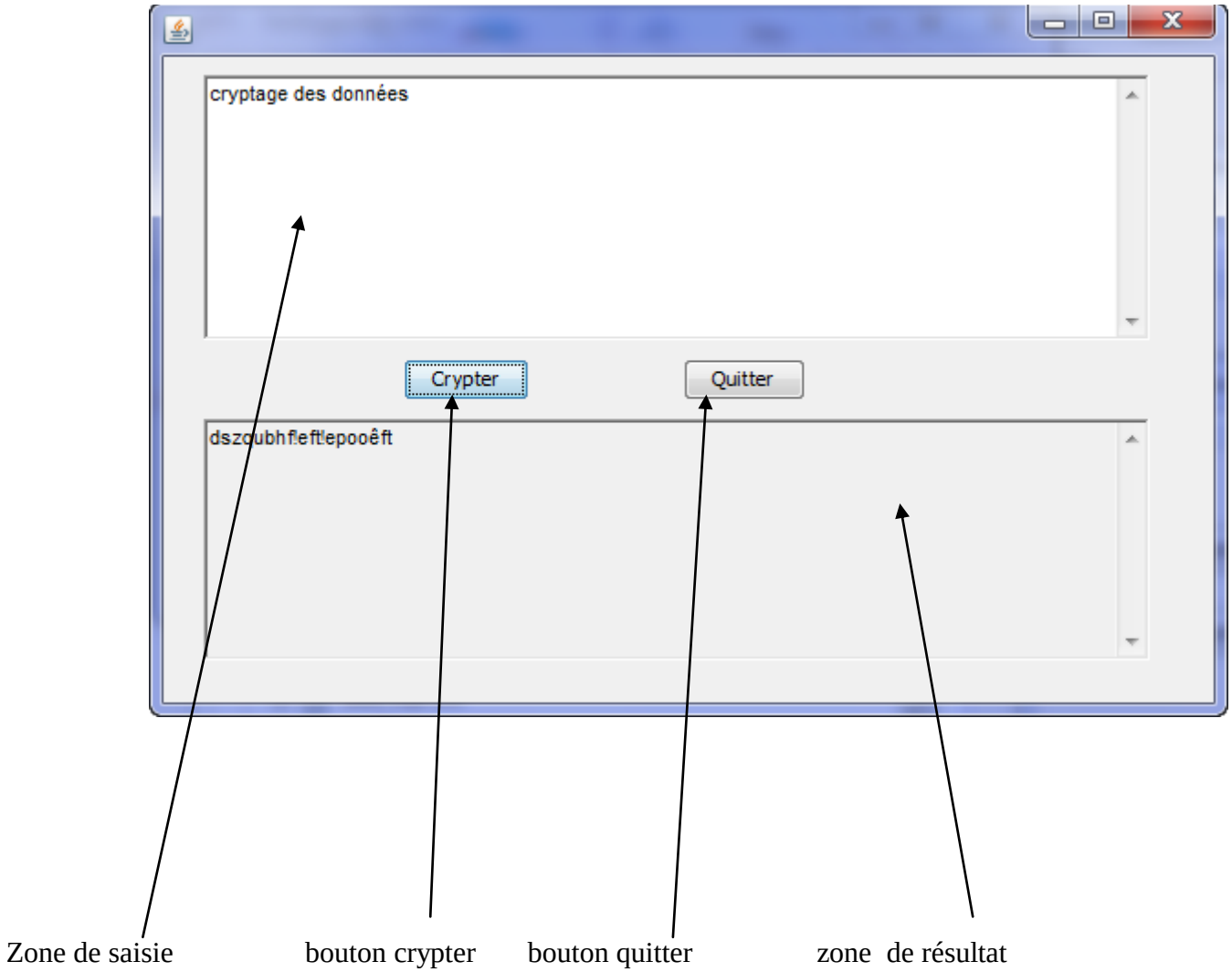


Figure 22: interface de cryptage par saisie

- **Zone de saisie** : nous offre la possibilité d'écrire un texte, et de faire appel a l'algorithme de cryptage a travers le bouton « crypter » et renvoyer le texte crypté dans la zone de résultat.
- **Bouton « quitter »** : permet de quitter la fenêtre.

e) Interface de décryptage :

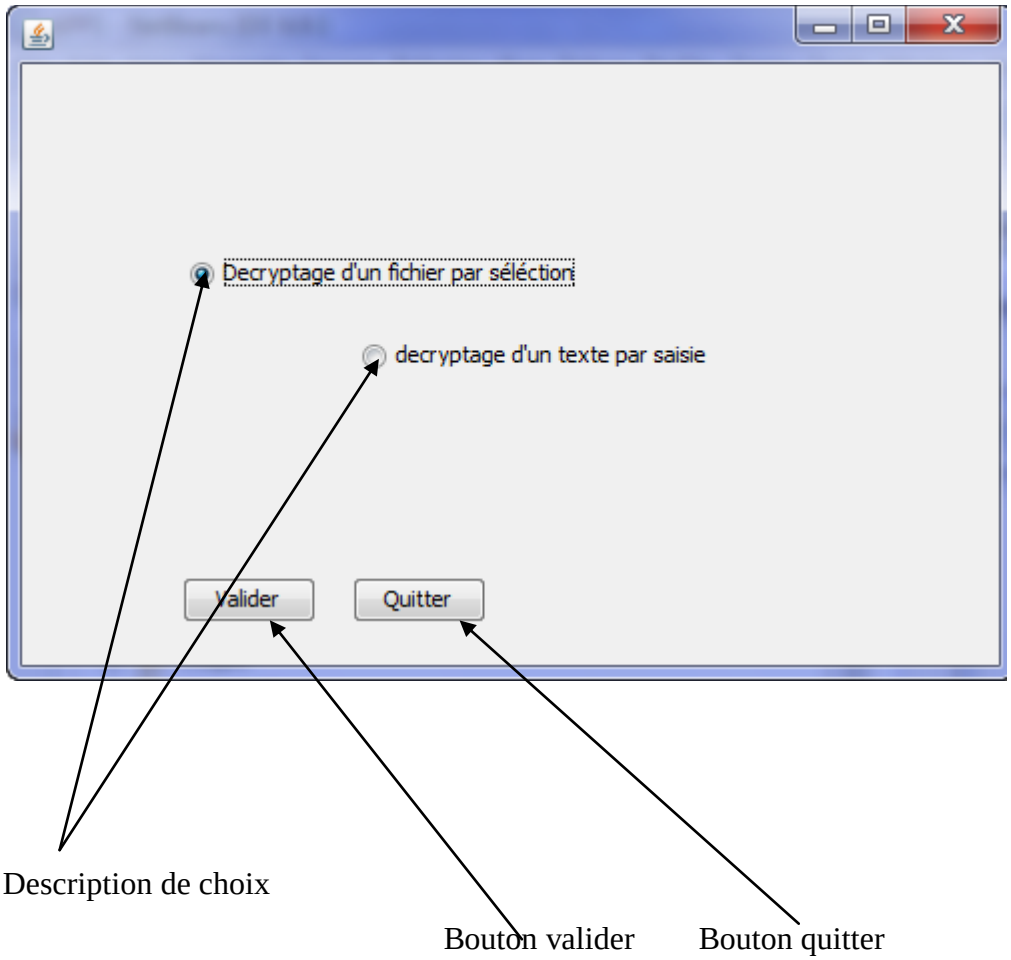


Figure 23: Interface choix de type de décryptage

- **Description de choix** : permet de choisir le type de décryptage,

Si l'utilisateur a choisi le décryptage par sélection de fichier il aura la figure pour choisir le fichier souhaité, sinon il aura la figure qui lui permettre de décrypter avec saisie de texte. Pour quitter l'interface de décryptage, l'utilisateur clique sur le bouton « quitter ».

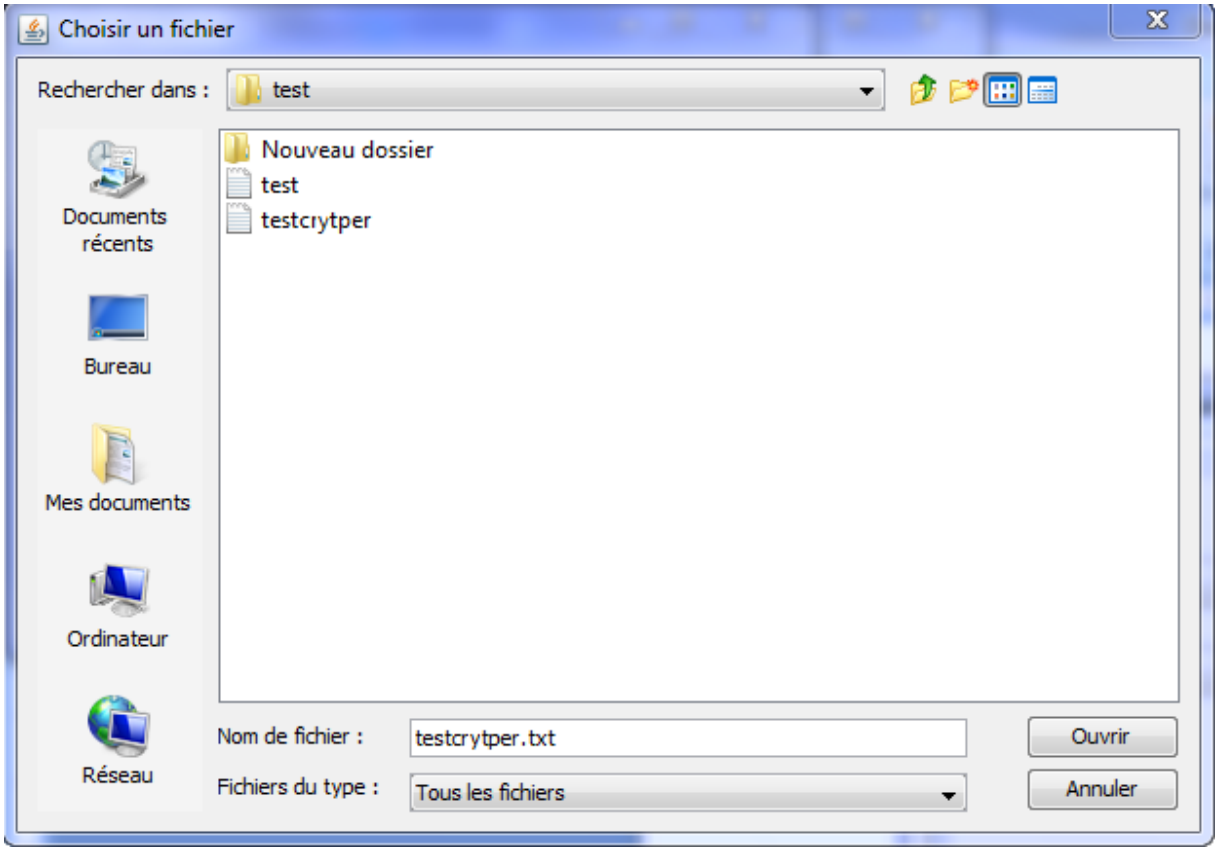


Figure 24: interface de sélection de fichier a décrypté

f) Interface de décryptage d'un fichier :

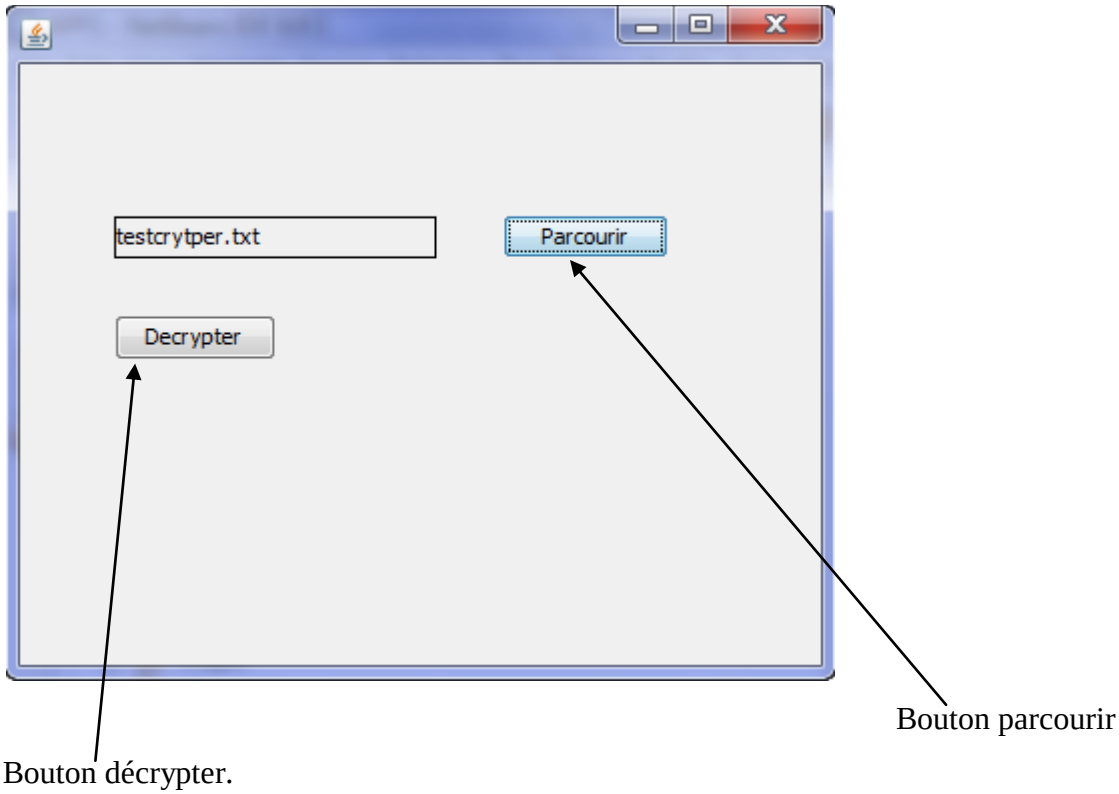


Figure 25: interface de sélection de fichiers à décrypter

- **Bouton « parcourir »** : permet de sélection le fichier a crypter.
- **Bouton « Décrypter » :** fait appel a l'algorithme de décryptage.

g) Décryptage de textes par saisie :

Cette interface offre la possibilité de saisir un texte dans la zone « saisie », et de décrypter en cliquant sur le bouton « décrypter ».Le texte décrypté apparait dans la zone résulat.

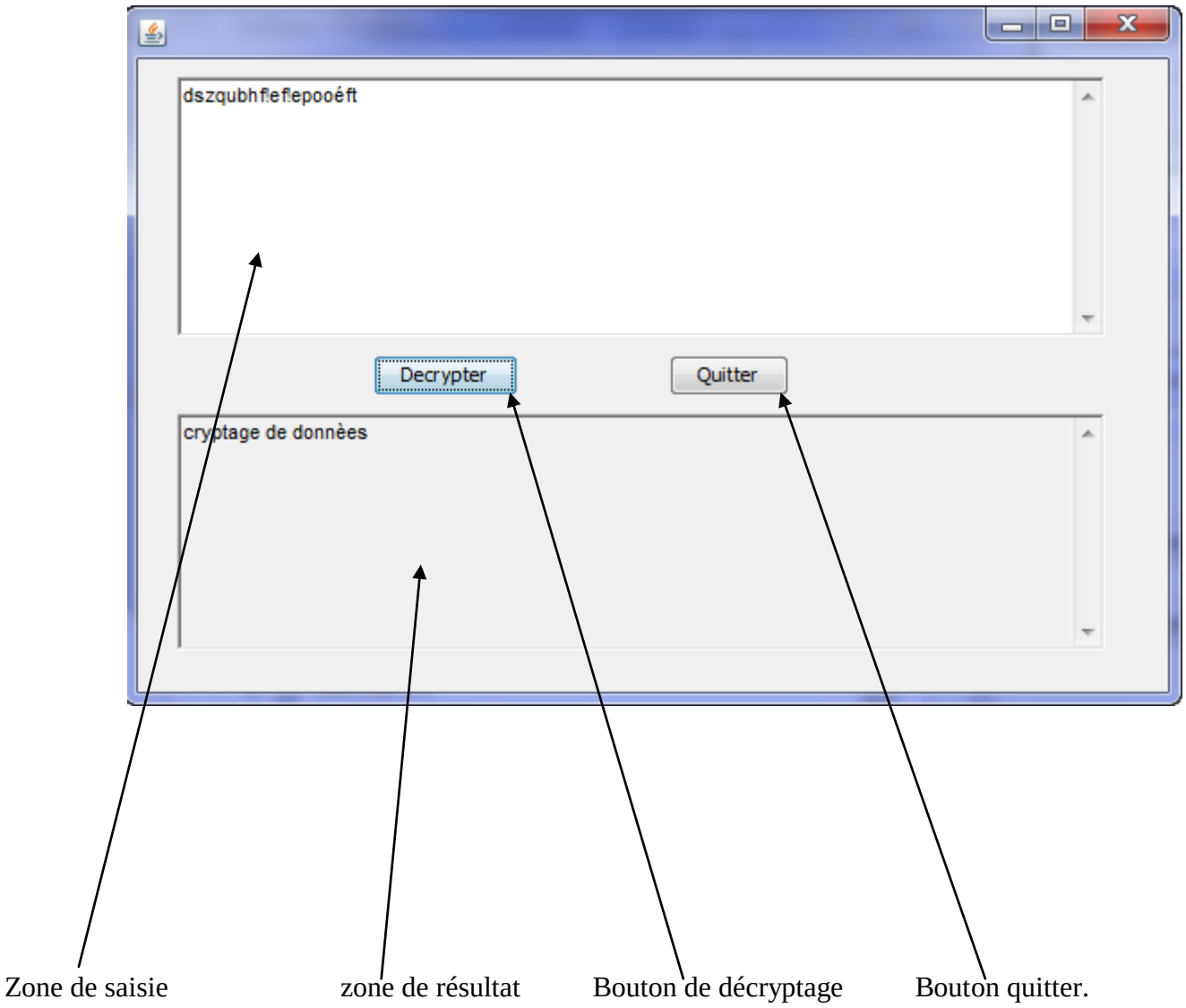


Figure 26 : interface de décryptage de texte

4.5. Conclusion :

Dans ce chapitre, nous avons présenté l'environnement d'implémentation et de développement de notre projet. Ainsi que les interfaces de notre application.

Conclusion Générale:

Le travail que nous avons mené nous a permis de nous ouvrir en premier lieu sur le domaine de la cryptographie et également sur d'autre domaine tel que la programmation orientée objet sous Windows.

Il nous a par ailleurs permis de nous familiariser avec les concepts et les algorithmes relatifs au cryptage de donner.

On a pu entreprendre le fonctionnement de la Machine Enigma, sa complexité de fonctionnement ainsi que le complexité de casser un code issu de son algorithme de cryptage.

Enfin, nous espérons avoir atteint l'Objectif de notre travail, pour les perspectives, nous espérons pouvoir implémenter plusieurs versions de la machine.

Bibliographie

[01] : fichier PDF : Tout sur la sécurité informatique 2ème édition de jean François Pilon et Jon-Philipe Bay. Dunas-paris 2005

[03] : fichier PDF : Sécurité informatique : principes et méthodes ; Laurent Blochet Christophe Wolfhugel, ÉDITIONS EYROLLES Paris Cedex 2007

[04] mémoire : Cryptographie et méthode de cryptage (mémoire IG. Etat électronique option communication (201/42).

[05] : Cours de Cryptographie (version préliminaire 2005/2006) Daniel Barsky (février 2006

[06] fichier PDF : Technique de cryptographie, Jonathan Blanc, Adrien De Georges, Licence informatique (2003 /2004).

[08] fichier PDF : Enigma et la seconde guerre mondiale Guillaume Munch et julien milli Aout 2004.

[02] :www.securiteinfo.com

[07] :http://www.commentcamarche.net